FPI ADVOCACY BRIEF

FEMINIST PRINCIPLES OF THE INTERNET:

PRIVACY AND DATA

PRINCIPLE ON PRIVACY

“We support the right to privacy and to full control over personal data and information online at all levels. We reject practices by states and private companies to use data for profit and to manipulate behaviour online. Surveillance is the historical tool of patriarchy, used to control and restrict women’s bodies, speech and activism. We pay equal attention to surveillance practices by individuals, the private sector, the state and non-state actors.”

ABOUT THE FEMINIST PRINCIPLES OF THE INTERNET (FPIS)

The Feminist Principles of the Internet (FPIs) are a number of principles that articulate an evolving set of concerns in relation to the internet and human rights, with a special focus on how gender and sexuality are located in diverse communities' experiences of the internet. They were drafted over a series of feminist gatherings. The first of these was called "Imagine a Feminist Internet", and took place in Malaysia in April 2014. The meeting was organised by the Association for Progressive Communications (APC) and brought together 50 activists and advocates working in the fields of sexual rights, women's rights and gender equality, violence against women/gender-based violence, and digital rights. The meeting was designed as an adapted open space where topics were identified, prioritised and discussed collectively.

A group of volunteers from the meeting drafted version 1.0 of the FPIs. This was subsequently brought to different workshops and events, local and global, and then to a second "Imagine a Feminist Internet" meeting in July 2015, where a new group of 40 activists discussed, elaborated on and revised the FPIs. The new version was published on the feminist internet website in August 2016, where anyone can expand the principles by contributing resources, commenting, or offering localised translations.

Currently there are 17 principles, organised into five clusters: Access, Movements, Economy, Expression and Embodiment. A new cluster on Care and the Environment is planned for 2022. Together, they aim to provide a framework for movements working to advance gender justice and human rights, to articulate and explore issues related to technology through a feminist lens.

For more information on FPI-related events, click here.
For Frequently Asked Questions, click here.
Get in touch with us here.

WHAT IS THE RIGHT TO PRIVACY ONLINE?

The right to privacy is essential to the free development of an individual's personality and identity. The human right to privacy is a limit on the exercise of power whether of states or non-state actors. By enabling personal choice, association and expression, and by protecting civil and socioeconomic freedoms and equality, privacy can help secure the political rights of women and gender-diverse people to participate in public and cultural life, fully and without hindrance.

Privacy also equips us to make decisions and establish boundaries on our own bodies and personal data. It allows us to limit others' access to our personal space/s, and strengthens autonomy, empowering each of us to use information about ourselves in ways which enable our own safety and security.

Privacy also delineates a space in which we can explore, experiment, express and think freely without judgment or discrimination. Privacy, and tools for privacy, such as encryption and other forms of anonymity, are essential for those marginalised in society by law, practices, norms and structures.

Online privacy is valuable to women, girls and gender-diverse persons as online spaces are spaces to connect with others, strengthen networks, derive pleasure, seek and produce knowledge, and express oneself. It becomes particularly important for women human rights defenders (WHRDs), feminist activists and organisers to safely and securely seek,

receive and impart information, to mobilise in advocacy of rights, and to connect and convene with rights defenders, community members and other stakeholders.

WHAT ARE THE RISKS TO PRIVACY ONLINE?

The right to privacy can be undermined online in myriad ways, including through surveillance; by the mass collection, storage and use of personal data by internet platforms; and by attacks by individuals that weaponise the collection, publication and dissemination of personal information, data and images against women, girls and gender-diverse persons.

WHRDs, feminist activists and journalists (with women journalists disproportionately impacted) are regularly subjected to surveillance and have their privacy rights persistently violated online. This is also the case for members of minoritised, criminalised or otherwise marginalised communities, such as sex workers and sexually and gender-diverse persons.[1] This means that their information and communications technology (ICT) devices may be tracked and hacked, for example, through the use of software designed to spy, and their online activity may be monitored, for instance, on social media. Their private communications or personal details, such as their home address, could be published on public forums – a practice known as doxing or doxxing.[2]

---

1. Cannataci, J. (2019). *Privacy and technology from a gender perspective: Report of the Special Rapporteur on the right to privacy*. A/HRC/40/63. https://www.ohchr.org/en/documents/thematic-reports/ahrc4063-privacy-and-technology-gender-perspective-report
2. In her 2018 report to the Human Rights Council (A/HRC/38/47), the UN Special Rapporteur on violence against women stated: "'Doxing' refers to the publication of private information, such as contact details, on the Internet with malicious intent, usually with the insinuation that the victim is soliciting sex (researching and broadcasting personally identifiable information about an individual without consent, sometimes with the intention of exposing the woman to the 'real' world for harassment and/or other purposes). It includes situations where personal information and data retrieved by a perpetrator is made public with malicious intent, clearly violating the right to privacy."

These attacks on privacy can be carried out by the state, or state-sanctioned actors such as groups of citizens allied with conservative state agendas; but they may also be carried out by private actors, family members and others known to the victims.

Many girls and women are at risk of having their personal data, including their images, intimate or otherwise, stolen and shared publicly without their consent – known as non-consensual dissemination of intimate images (NCII) – in acts of targeted technology-facilitated gender-based violence. Leaked images have also been used to create fake or deepfake imagery.[3]

This tends to happen more frequently with women, girls and gender-diverse people who are seen to be disruptors of social norms, including gender and sexual norms. These types of attacks rely on an already established foundation of gender-based violence and discrimination, stigma around sexuality, sexism, homophobia, transphobia and other social harms.

Although privacy breaches affecting women are nothing new, tech-facilitated erosion of privacy takes place today at an unprecedented pace. Internet-based platforms, including search engines, social media and other apps, indiscriminately collect data from their users through different strategies: sign-up/ registration processes, quizzes, games, etc. This data is not only frequently collected without authorisation – or sometimes even without the knowledge of users – it is also stored without minimum standards of transparency or safety, and often resold or repurposed.

---

3. As an example, see the case of Ghada Oueiss: https://cpj.org/2021/02/ghada-oueiss-hacking-harassment-jamal-khashoggi

In today's data-driven economy, huge amounts of data mean knowledge: insights into consumer behaviour, emerging market trends, or even predictors of the future. The growing field of artificial intelligence (AI) pushes this market to continue to collect more and faster, and find "innovative" ways to derive value from data.

Retail information, health records, work records, police records and others are useful data to profile and sell to advertising companies. Privacy harms can originate in business models, which makes it crucial to increase transparency on how private companies are using sensitive data. Platforms have a responsibility to inform users of their specific risks and create features that can mitigate those risks.

An example of misuse of data is the ability of apps to monitor, localise and even send specific propaganda to women and girls who are in the process of seeking an abortion, from the time when they are considering it and checking into their options or even when they are in an abortion clinic waiting room.[4]

The erosion of the right to privacy for girls, women and gender-diverse persons also has social, community and family dimensions to it. For example, in a household, privacy with technology may be granted to men and boys and not to women and girls, whose use of online tools or technological devices may be closely surveilled and restricted by other members of the

4. Coutts, S. (2016, 25 May). Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits. *Rewire News*. https://rewirenewsgroup.com/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits

family. In intimate relationships, young women and girls may be coerced into sharing passwords for social media accounts by intimate partners.[5]

Data processing never takes place in a gender-neutral manner, and the practices of internet platforms are no exception. A clear example is the recording, tracking and gathering of data on sexual and reproductive behaviours by corporations through period tracking apps. Although these apps may portray themselves as positive services, they are also new models of surveillance – self-surveillance – and thereby new models to define what is within the norm and what is not.

As the NGO Coding Rights has observed, these apps are ruled by a particular world view, normally run by men, with a particular vision of what women's role is, and "these men and their world view define the terms around what will be measured and why and whom will be measured and how."[6] Thus, the data gathered and shared with third parties may generate algorithms with the potential to create "new standards for reproductive and gynecological indicators based only on those women who have access to these apps, and those who bother to use them."[7] These mechanisms may give rise to the formation of new normative ideas around health and reproduction that affect women's bodies.

---

5. Kamra, D. (2012, 3 December). Love me? Then give me your password! *Times of India*. http://timesofindia.indiatimes.com/articleshow/11638410.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
6. Felizi, N., & Varon, J. (2016). *Menstruapps – How to turn your period into money (for others)*. Coding Rights. https://chupadados.codingrights.org/en/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros-2
7. Rizk, V., & Othman, D. (2016). Quantifying Fertility and Reproduction through Mobile Apps: A Critical Overview. *ARROW for Change, 22(*1). https://www.arrow.org.my/wp-content/uploads/2016/08/AFC22.1-2016.pdf

WHAT IS THE IMPACT OF THE EROSION OF PRIVACY?

Surveillance and privacy breaches create especially unsafe, hostile environments for women, girls, feminist activists and sexually and gender-diverse persons, and contribute to violence and harassment against these groups. This is primarily due to pervasive histories of gendered surveillance as a patriarchal tool of control, used against groups who are seen as disrupting social norms and social order, and the over-emphasis placed on policing girls' and women's bodies through their constant surveillance.[8]

Invasions of privacy on high-profile women, WHRDs, sex workers, feminist activists, and those perceived as challenging societal gender and sexual norms discourage girls, women and other marginalised people, such as gender-diverse persons, from public and political participation, imposing a chilling effect on freedom of expression.

Violations of the right to privacy online can have other dire material consequences on the lives of individuals, including risks to physical safety, such as violence and harassment, arbitrary detention, restrictions on freedom of movement and freedom of association, loss of employment and educational opportunities, vulnerability to fraud, extortion and reputational damage, negative mental health impacts, and even death.

8. Kovacs, A. (2020, 27 May). When our bodies become data, where does that leave us? *Deep Dives*. https://deepdives.in/when-our-bodies-become-data-where-does-that-leave-us-906674f6a969

Additionally, the gathering and processing of mass data, including on an individual's behaviour, interests, relationships, appearance and identity, can reinforce social and structural inequalities and discrimination, particularly when employed for identification, tracking, profiling, facial recognition and behavioural prediction, whether for commercial gain or state surveillance. Individuals in this case are not given the information needed, nor the opportunity in many cases, to provide free, explicit and informed consent to the collection, processing, storage and sale of their personal data for various purposes.

Some stakeholders, due to different interests, tend to present a false dichotomy between protecting the right to privacy, on the one hand, and exercising the right to free expression and to public and political participation, on the other. In order to evade accountability, corporations and state actors also create hierarchies of persons and groups with regard to privacy online, thereby indicating that some groups' right to privacy, freedom of expression or other rights are more important and in need of greater protection than others'.

WHAT IS THE IMPORTANCE OF ANONYMITY ONLINE?

The right to anonymity is an essential facet of privacy in the online context, especially for young women and girls, sex workers, WHRDs, sexual and gender-diverse persons and/or other criminalised or targeted groups. Encryption tools and privacy protocols foster freedom of expression, association and assembly by enhancing the safety and security of the online environment.

Many state actors have made significant efforts to oppose and block privacy tools such as the use of encryption or anonymity, and some intermediaries do not allow for anonymous use of their services, while severely jeopardising users' right to encryption and privacy through their own practices.

The policies of intermediaries and states around anonymity are a significant concern for the privacy and freedom of expression of girls, women, gender-diverse persons, sex workers, WHRDs and feminist activists, and other communities at high risk for surveillance, criminalisation and penalisation. Many intermediaries and platforms require users to disclose their identities (e.g. Facebook's "real name" policy), and sometimes even to provide copies of identity documents to use their platforms.

For sexually and gender-diverse persons, for example, this may lead to criminalisation for their sexual orientation and/or gender identity; depending on the context, this may also be the case for sex workers, migrants, refugees, asylum seekers and many others.

Women, girls, WHRDs and feminist activists including sexually

and gender-diverse persons may use anonymous online profiles, for example, to evade family surveillance, community surveillance or state surveillance, to escape family and/or intimate partner violence, to build community with supportive networks and groups, or to engage safely in online campaigning or political organising, and therefore can be adversely affected by these policies.

Poor privacy policies or practices can also be weaponised against them by their opponents (e.g. forced “outing” or the threat of being “outed”, being reported on platforms like Facebook for possessing “fake” profiles, etc.).

Digital anonymity allows sexually and gender-diverse persons, WHRDs and other targeted, criminalised or otherwise marginalised groups to seek information, find solidarity and support, and share opinions without fear of being identified. Anonymity provides a layer of security for feminist actors and WHRDs to engage in online spaces, and to communicate and campaign with reduced fear of backlash.

See the FPI on Anonymity for more information on this principle.[9]

9. https://feministinternet.org/en/principle/anonymity

IS PRIVACY PROTECTED BY INTERNATIONAL HUMAN RIGHTS NORMS AND STANDARDS?

The right to privacy is enshrined in the Universal Declaration of Human Rights (UDHR), which all UN member states have a responsibility to uphold. It is additionally included as a human right in the International Covenant on Civil and Political Rights (ICCPR).

Article 12 of the UDHR and Article 17 of the ICCPR provide that "no one shall be subjected to arbitrary or unlawful interference with his [or her] privacy, family, home or correspondence, nor to unlawful attacks on his [or her] honour and reputation." They further state that "everyone has the right to the protection of the law against such interference or attacks."

General Comment No. 16 (1988) of the Human Rights Committee on the right to privacy[10] states that surveillance, whether electronic or otherwise, should be prohibited. It additionally states that compliance with article 17 of the ICCPR requires that the integrity and confidentiality of correspondence should be guaranteed *de jure* and *de facto*, and that correspondence should be delivered to the addressee without interception and without being opened or otherwise read. The Committee further called upon states to take effective measures to prevent the unlawful retention, processing and use of personal data stored by public authorities and business enterprises.

10. https://www.refworld.org/docid/453883f922.html

WHAT HAVE THE INTERNATIONAL HUMAN RIGHTS MECHANISMS SAID ON THIS ISSUE?

UN human rights mechanisms have drawn attention to these issues, demonstrating ways in which international human rights standards can be applied to questions of privacy, data and surveillance in the digital sphere. The mechanisms are increasingly calling on duty bearers to respond to online harassment, the public dissemination of personal information or images, and the surveillance of human rights defenders and marginalised groups.

The Committee on the Elimination of Discrimination Against Women (CEDAW) has expressed concern on these issues, including on the dissemination of intimate content without consent;[11] the online harassment and abuse of women advocating for women's rights;[12] and the online publication of the names of victims and witnesses in proceedings for protection orders, preventing women from seeking justice for gender-based violence and discrimination.[13]

Reports and resolutions from the UN Human Rights Council (HRC) have been continuously addressing privacy and surveillance. For example, the HRC in its 2019 Resolution

11. CEDAW Concluding observations on the eighth periodic report of Indonesia 2021. CEDAW/C/IDN/CO/8. https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CEDAW%2FC%2FIDN%2FCO%2F8&Lang=en
12. CEDAW Concluding observations on the eighth periodic report of Australia 2018. CEDAW/C/AUS/CO/8. https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=CEDAW/C/AUS/CO/8&Lang=E
13. CEDAW Concluding observations on the combined seventh and eighth periodic reports of Romania 2018. CEDAW/C/ROU/CO/7-8. https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Download.aspx?symbolno=CEDAW%2FC%2FROU%2FCO%2F7-8&Lang=en

42/15 on the right to privacy in the digital age called on states to respect and protect the right to privacy, including in the context of digital communications where this pertains to procedures, practices and legislation regarding the surveillance of communications. The Council further called on states to "develop or maintain and implement adequate legislation, with effective sanctions and remedies, that protects individuals against violations and abuses of the right to privacy, namely through the unlawful or arbitrary collection, processing, retention or use of personal data by individuals, Governments, business enterprises and private organizations."[14]

Moreover, the Human Rights Committee, tasked with monitoring implementation of the ICCPR, has similarly called on multiple states in concluding recommendations to ensure that "[a]ll types of surveillance activities and interference with privacy, including online surveillance, interception of communications, access to communications data and retrieval of data, are governed by appropriate legislation that conforms with the Covenant, in particular article 17, and with the principles of legality, proportionality and necessity;" and that "[s]urveillance and interception activities are conducted subject to judicial authorization and to effective and independent oversight mechanisms and that the persons affected have proper access to effective remedies in cases of abuse."

14. Resolution adopted by the Human Rights Council on 26 September 2019: The right to privacy in the digital age. A/HRC/RES/42/15. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/297/52/PDF/G1929752.pdf?OpenElement

Similarly, the UN Special Rapporteur on the right to privacy has provided additional context to the impact of surveillance and the need for protection of the right to privacy from a gendered perspective in a 2019 report to the Human Rights Council,[15] noting the unique impact of harmful technologies, law and policy that erode the right to privacy for women, young sexually and gender-diverse persons and intersex persons who experience invasion of privacy and autonomy from birth. The report describes how newer dimensions of domestic violence include technology-facilitated invasion of privacy, as well as other forms of gender-based violence exacerbated or facilitated by technology, such as the non-consensual sharing of intimate imagery, which the Special Rapporteur found was more likely to affect sexually and gender-diverse persons. The mandate illustrated gender bias in surveillance, for example, through the facilitation of surveillance of LGBTQI communities through legislation, and the disproportionate impact of counter-terrorism measures on women and trans asylum seekers, refugees and immigrants. These troubling measures are not limited to sweeping state surveillance. The report also highlighted: "Women can expect that nearly every detail of their intimate lives will be subject to multiple forms of surveillance by State as well as private actors."[16]

We have compiled a more comprehensive listing of selected annotations concerning privacy from international and regional agreements and statements to support you in your policy advocacy endeavours.

15. Cannataci, J. (2019). Op. cit.
16. Ibid.

WHAT DUTIES DO STATES AND OTHER STAKEHOLDERS HAVE TO ADDRESS THIS ISSUE?

States have a duty to promote and protect the right to privacy in the digital sphere, to prohibit surveillance, and to take effective measures to prevent the unlawful retention, processing and use of personal data.

In addition, states have a duty to exercise due diligence to prevent, document and report gender-based violence including and resulting from unlawful and unjust breaches of privacy, including those committed online or through technology, and to ensure fair and equal access to justice and remedy for women, girls, gender-diverse persons, and criminalised or otherwise marginalised groups. States have a responsibility to hold actors who violate women's, girls' and gender-diverse persons' right to privacy, online or otherwise, to account, including and especially when they are state actors, state-sanctioned actors or allies of the state agenda. Data protection frameworks must be gender-responsive. Their design and implementation must consider gendered realities of the society we live in and ensure that injustices are not replicated as we race towards digital development.

When it comes to digitised social welfare programmes, beneficiaries, including women, should not have to choose between privacy and social protection, food security, or a benefit that after all alleviates but does not eliminate poverty.

Inferences generated by big data should be limited to safeguard people's autonomy of choice and freedom. Sensitive information should not be used to the detriment of the person, or to infer personal information, including their religion or sexual orientation. Reversing individual and collective attitudes that perpetuate patriarchal control and abuse of personal data and violations of the right to privacy on the basis of gender requires involving more women and LGBTQI+ people in the design, development and regulation of digital technologies. This is not simply a matter of representation; having a more diverse and inclusive range of people contributing to the design, development and regulation of the technologies will mean that questions, concerns and considerations about the implications of privacy on these individuals and groups will arise as well as solutions to safeguard their privacy (rather than overlook or dismiss such concerns). Promoting greater gender diversity among the people shaping online experiences is a shared responsibility of the state and the private sector.

Human rights bodies and mechanisms should also be encouraged to include the right to privacy in the digital sphere as relevant to their mandates in their work, research, missions, reports, communications and recommendations, providing guidance to states and other stakeholders in addressing this issue.

States can implement the recommendations of the human rights mechanisms, including UN Special Rapporteurs in areas such as the right to privacy and violence against women, in their reports addressing this theme. This includes acting in accordance with

the principle of due diligence to enact new laws and measures to prohibit new emerging forms of technology-facilitated gender-based violence, protect the right to privacy for all persons, and ensure that regulations on internet intermediaries respect the international human rights framework.

WHAT SHOULD INTERMEDIARIES DO?

Corporations should implement the UN Guiding Principles on Business and Human Rights,[17] and avoid infringing the human rights of all persons affected by their practices, with effective consideration of the gendered impact of their activities on women, girls and gender-diverse persons, criminalised groups, and other marginalised persons.

Intermediaries should ensure that respect for the right to privacy is incorporated into the design and purpose of their technologies, and provide compensation for human rights abuses that they have caused or to which they have contributed, along with other measures of accountability and greater transparency in decision making.

They should practise transparency with regard to how they use the personal data of users, taking steps to be in line with ethical standards and human rights standards, and prioritising human rights over profit. Corporations should respond carefully and thoroughly to reports of online gender-based violence, harassment, targeted campaigns, invasions of privacy and surveillance, and ensure adequate steps are taken. Greater diversity among those shaping and designing technologies, and policies towards their governance and management, is important for making products and platforms safer, more socially responsible and accountable.

---

17. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

Intermediaries can demonstrate leadership by upholding and applying international human rights standards in relation to gender-based violence, adopting transparent complaint mechanisms for incidents of violence and ensuring that policies and procedures on these issues are easily accessible and transparent.

Intermediaries have a responsibility to exercise due diligence in the prevention of online violence, including through effective and non-discriminatory moderation. Intermediaries should publish clear and comprehensive content moderation policies and human rights safeguards against arbitrary censorship, and transparent review and appeal processes.

All relevant stakeholders should uphold the right to privacy through anonymity and encryption, which are critical in protecting privacy and the right to freedom of expression.

WHERE CAN I LEARN MORE?

Providing a gender lens in the digital age (APC)

HRC43: APC statement on privacy and gender

Gendering Surveillance (Internet Democracy Project)

A DIY Guide to Feminist Cybersecurity

Joint submission to the Global Digital Compact on gender (APC and others)

Published by the Association for Progressive Communications (APC) 2023

This publication was developed with support from the UK Government.