Submission by the Association for Progressive Communications (APC) on the issue of right to privacy in the digital age

May 2025

This submission aims to provide input for the drafting of the report to be prepared by the Office of the High Commissioner for Human Rights (OHCHR) and presented to the 60th session of the Human Rights Council in September 2025 on the issue of challenges and risks with regard to discrimination and unequal enjoyment of the right to privacy associated with the collection and processing of data, including those addressed in the resolution, to identify and clarify related human rights principles, safeguards and best practices, as requested by the Human Rights Council in its resolution 54/21. It addresses the "key questions and types of input/comments sought"' as per the call for inputs made available by the OHCHR.1

Key questions and types of input/comments sought

1. Scenarios and concrete examples of instances where the collection and processing of data by public and private entities, including in the context of the development and use of artificial intelligence, is associated with discrimination and unequal enjoyment of the right to privacy across the range of its dimensions;
2. Main factors that cause or contribute to such outcomes, including
    - Technological factors,
    - Specific forms of data collection and data processing,
    - Economic, political and social factors,
    - Legal, policy and institutional factors.
3. Resulting impacts on rights holders, including intersectional forms of discrimination;
4. Safeguards and best practices to address and prevent such adverse impacts, including
    - legislative and regulatory frameworks,
    - institutional frameworks, oversight and accountability/remedy mechanisms,
    - self-governance approaches by business enterprises,
    - human rights due diligence methodologies, and

[1] https://www.ohchr.org/en/calls-for-input/2025/right-privacy-digital-age

- data governance approaches and models, including approaches to prevent or mitigate data biases.

Note: Mentions to “our research” refer to the collective research developed and published by APC, partner organisations and coalitions. We acknowledge the corresponding collaborations in the cited sources.

1. Scenarios and concrete examples of discriminatory data collection and processing

Government surveillance and data collection

In Pakistan, government surveillance particularly impacts marginalised groups, with dire consequences for those already vulnerable. Our research highlights how "[Muslim] women human rights defenders, journalists, women from marginalised groups, and LGBTQIA+ individuals face heightened risks of privacy violations."[2] These violations often serve as gateways to other forms of violence and control.

In Tanzania, authorities have assembled surveillance teams explicitly to target LGBTQIA+ communities. In 2018, Dar es Salaam's governor announced "a 17-person strong surveillance team to track gay people," claiming his task force could "identify phones that have sexual contents and social media groups or texts that were promoting gay 'behavior or prostitution'."[3] This exemplifies how surveillance is weaponised against already marginalised communities. The targeting of activists and human rights defenders in Tanzania has escalated beyond digital surveillance to physical detention

[2] Association for Progressive Communications. (2025). *Submission by the Association for Progressive Communications to the Human Rights Council Advisory Committee on the issue of technology-facilitated gender-based violence against women and girls.* https://www.apc.org/en/pubs/submission-association-progressive-communications-human-rights-council-advisory-committee

[3] Ryakitimbo, R. (2018, 15 November). Melt down of protections for data and privacy in Tanzania for LGBTQIA and others. *GenderIT.org*. https://www.genderit.org/feminist-talk/melt-down-protections-data-and-privacy-tanzania-lgbtqia-and-others

and abuse. In May 2025, Ugandan lawyer and activist Agather Atuhaire and Kenyan activist Boniface Mwangi were detained by Tanzanian authorities after arriving to support opposition leader Tundu Lissu. Mwangi reported that both activists were tortured, with authorities acting on orders from a "state security" employee who ordered they be taken to a secret location for "Tanzanian treatment".[4] This demonstrates how surveillance systems create the infrastructure for broader human rights violations, as digital monitoring capabilities enable authorities to track, identify and subsequently target activists and their supporters across borders.

In Lebanon, surveillance practices disproportionately affect vulnerable populations. Privacy International, Social Media Exchange (SMEX) and the Association for Progressive Communications reported that militias and non-Lebanese forces operating outside central government authority frequently violated citizens' privacy rights, with various factions using informer networks and telephone monitoring to obtain information about perceived adversaries. The ability of non-state actors to conduct communications monitoring is extremely concerning given these activities are unregulated by law, which is heightened by the lack of safeguards to protect citizens' privacy.[5]

Welfare programmes and digital ID systems

In South Korea, government welfare programmes compromise the privacy and safety of domestic violence survivors. The 2013 Global Information Society Watch (GISWatch) report from Korea reveals that NGOs providing shelter to women survivors of abuse must "register women's personal information in the Integrated Social Welfare Network

[4] Reuters. (2025, 23 May). Tanzania releases Ugandan activist at border, Kenyan colleague alleges torture. *Reuters*. https://www.reuters.com/world/africa/tanzania-releases-ugandan-activist-border-kenyan-colleague-alleges-torture-2025-05-23/

[5] Privacy International, Social Media Exchange, & Association for Progressive Communications. (2015). *The Right to Privacy in Lebanon: Stakeholder Report, Universal Periodic Review, 23rd Session - Lebanon*. Privacy International. https://privacyinternational.org/advocacy-briefing/783/right-privacy-lebanon

(ISWN)" to receive government funding.[6] This policy has led to abusers tracking down survivors through government databases, putting women at severe risk.

In India, the Aadhaar biometric ID system presents particular concerns for abortion seekers. With the Digital Health Mission linking all individuals' health records to their Aadhaar numbers, abortion data will be digitised in centralised databases. This poses significant risks given "cyber attacks on India's digital health infrastructure are among the highest in the world" and major breaches of the Aadhaar database have repeatedly occurred.[7]

In Lebanon, the government launched an e-government initiative that included establishing a Unique Identity Number (UIN) and subsequently introduced biometric passports.[8] The identity card includes 10 fingerprints, palm prints and the holder's parents' names. The biometric passport contains a chip with data on the holder's identity, criminal history, fingerprints and facial recognition. Without a comprehensive data protection framework or robust constitutional protection of the right to privacy, these biometric systems operate in a complete legal void, failing to regulate and limit the purpose of biometric data collection. This creates potential for surveillance through profiling, data mining and big data analysis. The use of biometric technology raises significant concerns regarding misuse, fraud, misidentification, inaccuracies and exclusion. Additionally, the unregulated retention of this data creates risks of "function creep" (uses of biometric data for purposes for which it was not originally collected) and concerns about data safety.

[6] Rashid, S. (2013, 27 November). Korea: Women's privacy in danger through surveillance and leaking of private information. *GenderIT.org*. https://www.genderit.org/articles/korea-womens-privacy-danger-through-surveillance-and-leaking-private-information

[7] George, J., & Lakshané, R. (2022, 10 October). Lack of a data protection law puts Indian abortion seekers at risk. *GenderIT.org*. https://www.genderit.org/feminist-talk/lack-data-protection-law-puts-indian-abortion-seekers-risk

[8] Privacy International, Social Media Exchange, & Association for Progressive Communications. (2015). Op. cit.

Platform governance and private sector surveillance

Ride-sharing applications raise privacy concerns specific to women. In Pakistan, research by Digital Rights Foundation explores "the privacy policies of ride-sharing apps and how the companies can be held accountable," examining "critical privacy questions like how is their data being stored?" and "notions of urban surveillance, safer cities, and security for women."[9]

Additionally, period-tracking apps and other health applications collect intimate data from women while offering little transparency about usage. As observed by Coding Rights, these apps are typically "ruled by a particular worldview, normally run by men, with a particular vision of what women's role is, and 'these men and their worldview define the terms around what will be measured and why and whom will be measured and how.'"[10]

In Lebanon, concerning practices of mass data retention were implemented without adequate privacy safeguards.[11] In 2013, the Public Prosecutor's office ordered all internet service providers (ISPs) and some internet cafes to retain user data for a period of one year. The order specified retention of usernames, IP addresses, websites accessed, protocols used and user locations.[12]

---

[9] Baldo, B. (2019, 11 July). Visibility and secrecy: Data protection, privacy and gender in Pakistan. *GenderIT.org*. https://www.genderit.org/articles/visibility-and-secrecy-data-protection-privacy-and-gender-pakistan

[10] Association for Progressive Communications. (2023). *Feminist Principles of the Internet: Advocacy brief on privacy*. https://www.genderit.org/FPI-paper-on-privacy

[11] Privacy International, Social Media Exchange, & Association for Progressive Communications. (2015). Op. cit.

[12] As noted by the UN Office of the High Commissioner for Human Rights in its report on the right to privacy in the digital age (2014), "any capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy with a potential chilling effect on rights, including those to free expression and association." Office of the United Nations High Commissioner for Human Rights. (2014). *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights (A/HRC/27/37)*. https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

2. Main factors contributing to discriminatory outcomes

Technological factors

The architecture of digital systems frequently fails to incorporate safeguards for marginalised populations. As seen in the case of Aadhaar in India, centralised databases holding sensitive health information present fundamental vulnerabilities that disproportionately impact women seeking reproductive healthcare.[13] The vulnerability of centralised databases extends beyond government systems to private sector platforms that serve marginalised communities. In July 2020, hyperlocal delivery service Dunzo experienced a data breach affecting over 3.4 million users during coronavirus lockdowns, when many vulnerable populations relied heavily on such services. The breach exposed not only phone numbers and email addresses but also users' last known locations, phone types, last login dates and IP addresses. Given that the breach occurred during lockdown periods, it likely exposed many users' home addresses, creating particular risks for women and other marginalised individuals who depend on privacy for their safety. The company's delayed disclosure of the full scope of the breach – initially understating both the extent of compromised data and the number of affected users – demonstrates how inadequate corporate transparency compounds the privacy risks faced by vulnerable populations.[14]

Artificial intelligence (AI) systems process large amounts of data, posing serious privacy risks when used for "identification, tracking, profiling, facial recognition, classifying and behavioural prediction or the scoring of individuals," while reinforcing racial discrimination.[15] The Association for Progressive Communications, in their joint submission to the Global Digital Compact on

[13] George, J., & Lakshané, R. (2022, 10 October). Op. cit.
[14] Deep, A. (2020, 29 July). Dunzo breach affected over 3.4 million accounts. *MediaNama*. https://www.medianama.com/2020/07/223-dunzo-data-breach-update
[15] Association for Progressive Communications, Access Now, & ARTICLE 19. (2021, 25 January). To protect privacy in the digital age, world governments can and must do more. *APC*. https://www.apc.org/en/pubs/protect-privacy-digital-age-world-governments-can-and-must-do-more

gender, emphasises that "we are still seeing many algorithms that discriminate against women or do not take into account people of diverse genders and sexualities. This is because they are trained using biased data sets that fail to represent the diversity of contexts and people. [...] AI and emerging technologies are being designed by people and therefore, there are gender and other intersecting biases, including race biases."[16]

The deployment of sophisticated surveillance tools without appropriate safeguards introduces serious risks for marginalised groups. In Lebanon, researchers from the Citizen Lab at the University of Toronto discovered Blue Coat PacketShaper installations, technology that allows for the surveillance and monitoring of users' interactions on various applications such as Facebook, Twitter and Google Mail.[17] While such tools can be used for legitimate purposes like controlling bandwidth costs, they also enable filtering, censorship and surveillance. This is particularly concerning in a context where the government had been drafting regulations to control online content related to public morals.

Data collection and processing factors

Metadata collection and retention pose specific risks. The UN High Commissioner for Human Rights report cited in a joint civil society statement endorsed by APC notes that "metadata merits stronger protection than it currently enjoys under national legal frameworks" and that "the interception of data about a communication ('metadata') can be as sensitive as the interception of the content of a communication."[18]

[16] Association for Progressive Communications, et al. (2023). *Joint submission to the Global Digital Compact on gender*. https://www.apc.org/en/pubs/joint-submission-global-digital-compact-gender
[17] Privacy International, Social Media Exchange, & Association for Progressive Communications. (2015). Op. cit.
[18] Human Rights Watch. (2014, 11 September). Joint Civil Society Statement on Privacy in the Digital Age Submitted to the 27th Session of the UN Human Rights Council. http://www.hrw.org/node/129031

Unconsented data sharing between entities exacerbates risks. In South Korea, the government shares information between systems like the Integrated Social Welfare Network and National Education Information System, allowing abusers to track domestic violence survivors.[19]

Bulk interception of data without appropriate safeguards raises serious privacy concerns. In Lebanon, security agencies have sought blanket access to communication data of all citizens.[20] In 2012, the Information Branch of the Internal Security Forces (ISF) requested interception and retention of all SMS text messages sent in Lebanon over a two-month period, including 2G and 3G data subscribers' log files, IP addresses, usernames, phone numbers, addresses, names and passwords. In 2014, the government approved a proposal allowing the ISF unrestricted access to electronic communications data of all Lebanese citizens for six months, far exceeding the two-month limit permitted by Law 99/140. This bulk interception and access to data directly challenges principles of necessity and proportionality required when conducting activities that interfere with fundamental human rights.

A 2019 report from the UN Special Rapporteur on the right to privacy notes that inadequate privacy management in the context of name and gender changes in identity documents creates "deeply embarrassing and distressing privacy incursions for transgender individuals" during ordinary activities like travel, banking, and medical appointments.[21] The online availability of public records, judicial notices and decisions concerning gender identity were also identified as privacy concerns, especially when combined with big data and search engine capabilities.

[19] Rashid, S. (2013, 27 November). Op. cit.
[20] Privacy International, Social Media Exchange, & Association for Progressive Communications. (2015). Op. cit.
[21] Cannataci, J. (2019). *Report of the Special Rapporteur on the right to privacy*. https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session40/Documents/A_HRC_40_63.DOCX

Economic, political and social factors

Patriarchal power structures fundamentally shape privacy violations. APC observes that "surveillance is the historical tool of patriarchy, used to control and restrict women's bodies, speech and activism."[22] This manifests in how "many of the incidents of [technology-facilitated gender-based violence] begin with violation of privacy of the person being attacked."[23]

Religious and social conservatism often drives surveillance of women and LGBTQIA+ communities. In Tanzania, the governor justified surveillance of LGBTQIA+ individuals by stating, "I prefer to anger those countries than to anger God."[24] Following government announcements about surveilling gay communities, "LGBTQIA+ communities have reported feeling unsafe, scared and with nowhere to run to for support [...] leading to many hiding away" and "self-censoring themselves from using the internet and social media in fear of being traced."

A report on South Africa in a study published by the African Declaration on Internet Rights and Freedoms Coalition highlights how existing digital inequalities exacerbate discriminatory effects in data protection, creating a "data divide": "These truths about digital inequality do not, however, consider the full spectrum of experienced inequality. [...] The unaffordability of data, which is very consequential for lower-income groups usage, also means that 'most people are using services passively, not in the active, high-speed, always-on environment where studies of causality in relation to penetration and economic growth have been done.'" This passivity, connected to digital literacy, means that lower-income individuals accessing the internet "merely become a market for global digital commerce, rather than the beneficiaries of digital dividends." The report further notes that marginalised populations with less access and digital literacy not only have limited ability to exercise their data protection rights but are also more likely to be

[22] https://feministinternet.org/en/principle/privacy-data
[23] Association for Progressive Communications. (2025). Op. cit.
[24] Ryakitimbo, R. (2018, 15 November). Op. cit.

compelled to exchange their personal data for essential services, creating unequal power dynamics in data collection.[25]

In Lebanon, security agencies operate with minimal oversight or transparency. According to a Beirut-based media outlet, "all security services, without exception, continue to illegally operate their own wiretapping divisions of unknown nature and scope. [...] This means that there are no guarantees the security services are not eavesdropping on the Lebanese away from any legal oversight."[26] The competition between security services leads each agency to establish its own surveillance "centre" outside legal frameworks. These various security agencies fail to ensure that their policies and practices adhere to international human rights standards or adequately protect citizens' rights to privacy and freedom of expression.

An APC policy explainer on a human rights-based approach to cybersecurity critiques how "often cybersecurity policies, like national security policies, define security in relation to the state, rather than the people." It further emphasises: "A secure internet is best achieved through a rights-based approach and must centre on the security of users as opposed to the security of states."[27] This insight shows how institutional frameworks that prioritise state security over individual rights can create systems where marginalised communities' specific security needs are overlooked or sacrificed for broader national security concerns.

[25] African Declaration on Internet Rights and Freedoms Coalition. (2021). *Privacy and personal data protection in Africa: A rights-based survey of legislation in eight countries.* https://www.apc.org/sites/default/files/PrivacyDataProtectionAfrica_CountryReports.pdf

[26] Privacy International, Social Media Exchange, & Association for Progressive Communications. (2015). Op. cit.

[27] Association for Progressive Communications. (2020). *APC policy explainer: A human rights-based approach to cybersecurity*. https://www.apc.org/en/pubs/apc-policy-explainer-human-rights-based-approach-cybersecurity

Legal, policy and institutional factors

Weak or non-existent data protection frameworks enable discrimination. In Pakistan, "the absence of a legislative framework on privacy further poses a threat to people's freedoms to exercise their rights."[28]

Government exemptions from data protection requirements are particularly concerning. As noted in the case of Pakistan, the draft Personal Data Protection Bill "paradoxically exempts government bodies from compliance requirements" despite "extensive data collection, demonstrated security failures, and lack of oversight" creating "a perfect storm: state agencies can continue to gather, store and process personal data with minimal safeguards."[29]

The lack of robust constitutional protection for privacy creates an environment conducive to violations. In Lebanon, the constitution only protects the inviolability of the home, but fails to protect the secrecy of communications.[30] This constitutional oversight is particularly concerning given the extensive powers of the Lebanese government to conduct surveillance of communications. While Law 99/140 establishes that the right to secrecy of communications is protected and cannot be subject to any form of wiretapping or interception except in cases prescribed by law, systematic failures to abide by these legal safeguards directly threaten citizens' right to privacy.

Furthermore, Lebanon operates without a comprehensive data protection regime, creating a regulatory vacuum for handling sensitive personal information.[31] The country has proposed an e-transaction bill, but this remains in draft form and has been criticised for provisions that would allow warrantless search and seizure of financial, managerial

[28] Arora, S. (2023, 10 May). Researching and reflecting on experiences of digital privacy in India. *GenderIT*.org. https://www.genderit.org/articles/researching-and-reflecting-experiences-digital-privacy-india

[29] Kamran, H. (2025, 24 February). Between privacy and power: The fine line in Pakistan's Data Protection Bill. *GenderIT.org*. https://www.genderit.org/articles/between-privacy-and-power-fine-line-pakistans-data-protection-bill

[30] Privacy International, Social Media Exchange, & Association for Progressive Communications. (2015). Op. cit.

[31] Ibid.

and electronic files, as well as establishing a regulatory body with practically unchecked powers. Critics noted that the bill was not opened for public consultation, failing to allow civil society and other stakeholders to contribute to the law-making process.

The absence of specific protections for vulnerable groups in data protection laws is clear in multiple country-case studies. For example, as pointed out in a report from the African Declaration on Internet Rights and Freedoms Coalition, Uganda's Data Protection and Privacy Act "does not make any special mention of other vulnerable groups, such as persons with disabilities and the elderly. It only mentions the children whose data can be collected after seeking consent from their parents or guardians (section 8)."[32] Similarly, in Tanzania, the same report notes rising instances of gender-based violence online, and that women are often victims of privacy violations without adequate legal protection.[33]

3. Resulting impacts on rights holders

Intersectional forms of discrimination

Muslim women face compounded risks due to religious and gender discrimination. In India, one interview subject noted she felt grateful for having a Hindu name, as it would not reveal her identity as a Muslim woman, and protected her from violence and discrimination against minorities.[34]

LGBTQIA+ communities experience severe repercussions from privacy violations. In Tanzania, as noted earlier, following government announcements about surveilling gay communities, "LGBTQIA+ communities have reported feeling unsafe, scared and with

[32] African Declaration on Internet Rights and Freedoms Coalition. (2021). Op. cit.
[33] Ibid.
[34] Arora, S. (2023, 10 May). Op. cit.

nowhere to run to for support [...] leading to many hiding away" and "self-censoring themselves from using the internet and social media in fear of being traced."[35] Survivors of gender-based violence face life-threatening consequences when privacy is breached. In South Korea, there have been "examples where an abuser tracked down a survivor through either the ISWN, or, in the case of women who fled with their children, through the National Education Information System."[36]

Restrictions on anonymity and privacy-enhancing technologies disproportionately affect marginalised communities. In Lebanon, there have been unconfirmed reports of extralegal methods used to identify anonymous online users, with such incidents often remaining low-profile as individuals feel intimidated and threatened. When anonymity is challenged or undermined, citizens, particularly those speaking out against the government, have little or no protection from surveillance, facilitating government efforts to monitor and identify them. Additionally, certain voice over internet protocol (VoIP) applications are blocked inconsistently across internet service providers, with no clear or transparent policy for such decisions. While the government claims VoIP applications cause revenue losses, these applications typically provide more secure communications. When people are forced to use traditional phone lines, the government's ability to conduct surveillance increases.[37]

The UN Special Rapporteur on privacy's 2019 report notes that digital technologies have a considerable effect upon privacy by amplifying experiences of the non-digital world. The benefits of digital technologies are unequally available due to structural inequity and discriminatory gender norms that disproportionately affect women, non-binary gender and cis-normative individuals, the poor, and minority religious or cultural communities. The report specifically notes how cybermisogyny and general cyberabuse of individuals of non-binary gender are enabled by new technologies with "infinitely greater reach, durability and impact than previously."[38]

[35] Ryakitimbo, R. (2018, 15 November). Op. cit.
[36] Rashid, S. (2013, 27 November). Op. cit.
[37] Privacy International, Social Media Exchange, & Association for Progressive Communications. (2015). Op. cit.
[38] Cannataci, J. (2019). Op. cit.

An APC advocacy brief highlights that "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." These violations can lead to "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."[39]

4. Safeguards and best practices

Legislative and regulatory frameworks

Comprehensive data protection legislation should explicitly include protections for marginalised groups. Legislation must "establish explicit exemptions for actions that threaten fundamental rights and risk discriminating against marginalised communities."[40] Privacy legislation should require "proper safeguards for children's data, including mandatory age verification and parental consent requirements" while addressing specific risks to "oppressed groups and younger users from exploitation in an increasingly digitised landscape."[41]

For reproductive health data, regulations should "clearly identify the necessary and proportionate conditions for collecting, accessing, and storing data related to healthcare" and "define the conditions for which sensitive health data, such as abortion records, may be summoned by the state."[42]

[39] Association for Progressive Communications. (2023). Op. cit.
[40] Kamran, H. (2025, 24 February). Op. cit.
[41] Ibid.
[42] George, J., & Lakshané, R. (2022, 10 October). Op. cit.

In our recommendations to the government of Lebanon,[43] APC and partners emphasised the need to:

- Recognise and take steps towards compliance with international human rights law by ensuring the application of key principles to communication surveillance, including legality, legitimacy, necessity, adequacy, proportionality, and respecting due process with authorisation from competent judicial authorities.
- Investigate claims of illegal communications interception and data access by security services and other state authorities, ensure such practices are ended, hold responsible individuals accountable, and provide redress to victims.
- Ensure appropriate controls to prevent the use of private surveillance industry products to facilitate human rights abuses.
- Ensure that state surveillance of online and offline activities is lawful and does not infringe on human rights defenders' freedom of expression.
- Immediately enact data protection legislation that complies with international standards.
- Establish an independent data protection authority.
- Make further efforts to ensure freedom of opinion and expression, including by ensuring that blocked or filtered websites are based on lawful criteria.

The APC joint submission to the Global Digital Compact on gender recommends that governments "adopt an intersectional approach to understanding and protecting the right to privacy, which recognises the specific experiences and threats to privacy experienced by women and LGBTQI+ persons" and "make gender a key consideration of the development and enforcement of data protection frameworks."[44]

[43] Privacy International, Social Media Exchange, & Association for Progressive Communications. (2015). Op. cit.
[44] Association for Progressive Communications et al. (2023). Op. cit.

Institutional frameworks and oversight

Independent oversight bodies are essential. The Pakistan case study warns against oversight mechanisms "under federal government control" as this "enables selective enforcement which can potentially target critics and could allow state-aligned institutions to operate with impunity."[45]

Human Rights Council Resolution 42/15 calls upon states to "further develop or maintain preventive measures and remedies for violations and abuses regarding the right to privacy in the digital age that may affect all individuals, including where there are particular effects for women, and children and persons in vulnerable situations or marginalised groups." This highlights the need for targeted protections that address the specific vulnerabilities and impacts experienced by marginalised groups, recognising that a one-size-fits-all approach to privacy protections may not adequately address intersectional forms of discrimination and privacy violations.

Business self-governance and due diligence

Companies should implement the UN Guiding Principles on Business and Human Rights, "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."[46]

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."[47]

[45] Kamran, H. (2025, 24 February). Op. cit.
[46] Association for Progressive Communications. (2023). Op. cit.
[47] Ibid.

Data governance approaches

Data governance with a focus on human rights can benefit from an approach to cybersecurity as defined by our research as one that must be "systematic, meaning that it addresses the technological, social and legal aspects together."[48] This holistic framing suggests that effective prevention of discriminatory impacts requires integrated approaches across technological systems, social contexts and legal frameworks rather than treating these as separate domains.

Privacy-by-design principles are also crucial. As an APC statement on privacy and gender notes, "States and companies [should] adopt privacy by design/default and conduct gender impact analyses before the introduction of new products, services, legislation and other initiatives."[49] Meaningful participation of affected communities in technology design is essential. The same APC statement stresses that "meaningful engagement of women and LGBTIQ persons in the design and development of these policies and features is fundamental. [...] It is important to ensure that states and companies adopt policies and design with these groups rather than for these groups."[50]

The APC joint submission to the Global Digital Compact on gender specifically calls for "a presumption of algorithmic bias" to be considered when evaluating AI systems and recommends that "[e]quality-by-design principles, including human rights and gender rights impact assessments, should be incorporated into the development of any algorithmic decision-making systems or digital technologies prior to going to market, to prevent discrimination and harmful biases being amplified and/or perpetuated."[51]

[48] Association for Progressive Communications. (2020). Op. cit.
[49] Association for Progressive Communications. (2023, 11 September). HRC43: APC statement on privacy and gender. https://www.apc.org/en/pubs/hrc43-apc-statement-privacy-and-gender
[50] Ibid.
[51] Association for Progressive Communications et al. (2023). Op. cit.

Promoting gender and racial diversity in technology development is vital. As argued in the APC advocacy brief on privacy, "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."[52]

[52] Association for Progressive Communications. (2023). Op. cit.