Policy Brief

Safeguarding Digital Rights:

Policy Recommendations to Protect Structurally Silenced Women in Uganda from Surveillance, Privacy Violations, and Data Misuse

Aug 2025

APC

WOMEN AND ICTS WOUGNET WOMEN OF UGANDA NETWORK

Acknowledgements

The publication of this policy brief was made possible through the collective efforts of the WOUGNET team. Special recognition goes to Ms. Esther Nyapendi, Project Lead and Technical Support Officer, whose tireless work was carried out under the guidance of Ms. Sandra Aceng, Executive Director, and Mr. David Iribagiza, Program Manager, Information Sharing and Networking.

We are especially grateful to Mr. Moses Owiny for his invaluable technical support throughout the research process, as well as for his contribution to the drafting, review, and approval of this brief. We also extend our sincere appreciation to our partner, the Association for Progressive Communications (APC), for the generous financial and technical support provided under the Our Voices, Our Futures (OVOF) project.

This work contributes to strengthening women's voices by supporting their ability to shape inclusive online spaces, defend their rights, and engage fully in digital expression and advocacy.

Contents

List of Acronyms

AHA: Anti-Homosexuality Act, 2023
APC: Association for Progressive Communications
FGD: Focus Group Discussion
HRAPF: Human Rights Awareness and Promotion Forum
LGBQTI: Lesbian, Gay, Bisexual, Queer, Transgender, and Intersex
NITA-U: National Information Technology Authority-Uganda
OVOF: Our Voices, Our Futures
RICA: Regulation of Interception of Communications Act, 2010
UCC: Uganda Communications Commission
WHRD: Women Human Rights Defender
WOUGNET: Women of Uganda Network

1. Executive Summary

In Uganda, structurally silenced women, for instance, Women Human Rights Defenders (WHRDs), women with disabilities, sex workers, and gender diverse communities face severe digital rights violations through state-targeted surveillance, privacy breaches, data misuse, and network disruptions. Focus group discussions (FGDs) with 25 women reveal a pervasive climate of fear, distrust, and self-censorship driven by phishing attacks, digital coercion, and police demands for private data, with heightened concerns as the 2026 elections approach.

These violations, enabled by flawed laws such as the Regulation of Interception of Communications Act (RICA), 2010, and inadequate enforcement of the Data Protection and Privacy Act, 2019, undermine constitutional protections (Articles 21 and 27). The Anti-Homosexuality Act (AHA), 2023, exacerbates harm, with 9 documented LGBQTI evictions in May 2025 linked to discriminatory crackdowns.[1] Women's voices from FGDs, such as a WHRD's fear that "every call feels like a trap," and that they "always feel paranoid" and "unsafe both within and outside Uganda", underscore the urgent need for reform.

This brief proposes gender-inclusive legal reforms, mandatory court oversight for surveillance, digital literacy programs, and ethical guidelines for AI and biometrics to ensure safety and anonymity.

Recommendations are tailored for government (legal amendments), civil society (awareness campaigns), the private sector (ethical data practices), and agencies such as the Uganda Communications Commission (regulatory oversight). By amplifying the lived experiences of 25 women and aligning with Uganda's constitutional commitments and international standards, this brief calls for urgent collaboration to empower marginalised women and secure their digital rights.

---

1 *Human Rights Awareness and Promotion Forum (HRAPF). (2025). Report on violence and violations based on real or presumed sexual orientation or gender identity during the month of May 2025.*

2. Introduction

Uganda's escalating reliance on state surveillance, invasive data collection, and network disruptions disproportionately impacts structurally silenced women, including WHRDs, women with disabilities, sex workers, and gender diverse communities, eroding their safety, agency, and fundamental rights.

The 1995 Constitution guarantees equality under Article 21(1), ensuring that all persons are equal before the law in all spheres, including political, economic, social, and cultural spheres. Article 21(2) prohibits discrimination based on sex, disability, or other identities. Article 27 further protects privacy, barring interference with personal communications or property. However, these constitutional safeguards are undermined by a deeply patriarchal society that perpetuates unequal power dynamics, amplifying vulnerabilities in digital spaces.

An intersectional lens illuminates how gender, sexuality, and disability intersect to exacerbate digital discrimination. Online harassment, gendered disinformation, data breaches, and discriminatory laws like the AHA, 2023, disproportionately harm marginalised women, limiting their ability to engage in advocacy or public discourse.

For instance, FGDs with 25 women revealed that surveillance and phishing attacks create a "condition of fear," with one participant noting, "I stopped posting about my identity online; the state might use it against me because it's always the government that watches over us." Such experiences highlight the urgent need to address digital rights violations, particularly as political tensions rise ahead of the 2026 elections.[2]

25 women revealed that surveillance and phishing attacks create a ***"condition of fear"***

Purpose:

This policy brief analyses the gendered impacts of surveillance, privacy violations, and data misuse, drawing on legal analysis and FGDs with 25 structurally silenced women.

It proposes feminist-informed, actionable reforms to strengthen legal protections, enhance enforcement, and empower communities.

Scope:

The brief focuses on Uganda's legal framework and the lived experiences of WHRDs, women with disabilities, sex workers, and gender diverse communities, emphasising intersectional solutions to ensure digital safety and equality. It builds on WOUGNET's Our Voices, Our Futures (OVOF) project, supported by the Association for Progressive Communications (APC), to advocate for inclusive policies and practices.

2 *Media Legal Defence Initiative. (n.d.). Training manual on digital rights and freedom of expression online.*

3. Problem Statement

Structurally silenced women in Uganda, WHRDs, women with disabilities, sex workers, and LGBQTI communities face disproportionate harm from state-driven surveillance, privacy invasions, and data misuse, fostering intimidation, fear, and disempowerment. FGDs with 25 women reveal a hostile digital landscape characterised by pervasive distrust and paranoia, stifling their ability to engage in digital activism.[3]

Participants reported that state surveillance, often facilitated by telecommunications companies, monitors devices without consent, violating privacy rights enshrined in Article 27 of the 1995 Constitution. For example, a WHRD shared, "I can't trust my phone and my shadow; every call feels like a trap," and that "surveillance is a double-edged sword...they (government) tend to cover it up in issues of national security", reflecting the constant fear of being monitored. Phishing emails targeting activists have eroded trust within movements, with many WHRDs reporting hacked accounts after clicking malicious links, leading to data breaches and blackmail.

A participant recounted, "Fake profiles trick us into sharing personal messages, then they're used to shame us," highlighting digital entrapment tactics.

> ***"Fake profiles trick us into sharing personal messages, then they're used to shame us,"***

As the 2026 elections approach, interceptions of communications targeting marginalised groups and communities intensify, driving self-censorship among those who fear state surveillance. One participant added, "Oftentimes, we have seen the most marginalised communities like the gender diverse communities and the sex workers have had their communications intercepted."

Another participant expressed heightened digital insecurity, with one stating, "I stopped posting about my identity online; the state might use it against me." Women with disabilities face additional barriers, as one noted, "I avoid online platforms because I fear my data isn't safe, and I can't access secure tools."

> ***"I stopped posting about my identity online; the state might use it against me."***

These experiences confirm a pervasive climate of unsafety, particularly during politically sensitive periods, where digital activism is curtailed by fear of reprisal. A participant noted that during the election period, "people fear to comment and give opinions because they would be tracked down to their homes."

FGDs also revealed alarming instances of digital exploitation. Police have demanded passwords from WHRDs, sex workers, and gender diverse individuals to access private communications, confirming reports of digital entrapment.[4] A participant explained, "Police use our private messages to arrest us, saying we broke the law." Further corroborating findings from literature from the Human Rights body HRAPF.[5] State agents use fake social media or dating app accounts to lure activists into sharing romantic or explicit content, later used for prosecution or blackmail, creating a constant sense of being watched.[6]

Another participant described, "The feeling that the state is watching looms every day in our lives." These tactics not only violate privacy but also undermine the credibility and safety of structurally silenced women, perpetuating a cycle of fear and marginalisation.

---

3 Human Rights Awareness and Promotion Forum (HRAPF). (2025). Report on violence and violations based on real or presumed sexual orientation or gender identity during the month of May 2025.

4 ibid

5 ibid

6 Access Now. (2025). How Uganda's anti-LGBTQ+ laws entrap people online. https://www.accessnow.org (Accessed June 7, 2025)

The Ugandan state justifies surveillance technologies such as spyware, biometrics, and AI-driven facial recognition, initiated under operations like "Fungua Macho" as early as 2011, as necessary for crime prevention, public safety, and national security.[7] However, these measures often downplay their detrimental human rights impacts.

The UN Special Rapporteur on Freedom of Expression defines communication surveillance as the monitoring, interception, collection, and retention of data over communication networks, underscoring its invasive scope.

Structurally silenced women face technology-facilitated abuses, including misogynistic online hate speech, gendered disinformation targeting their sexual orientation, and non-consensual sharing of explicit images[8] (e.g., revenge porn). These abuses, as one WHRD noted, "destroy our credibility and make us live in constant fear," perpetuating gendered harm in Uganda's patriarchal society.

Evidence:

FGD Findings:

The 25 women emphasised a chilling effect on digital activism due to pervasive fear and distrust. A woman shared, "I avoid online platforms because I fear my data isn't safe, and I can't access secure tools," highlighting accessibility barriers.

Other participants reported self-censorship, with one stating, "I stopped posting about my identity online; the state might use it against me." Participants described digital entrapment, noting, "Police use our private messages to arrest us, saying we broke the law."

A WHRD recounted, "I learned that some of my colleagues were hacked after clicking a phishing email; now I'm scared of those emails" These testimonies confirm a hostile digital environment, particularly during politically sensitive periods like elections, where surveillance intensifies.

The women's collective fear of telecommunications complicity, as one participant noted, "Telecoms help the state spy on our calls and messages," underscores the need for systemic change.

Case Study:

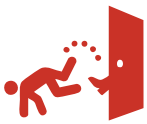
HRAPF documents harrowing experiences of digital entrapment, where fake social media accounts lured individuals into sharing personal messages, later used to blackmail them into silence, but also criminal prosecution. This case mirrors broader FGD findings, where women reported similar tactics, particularly targeting sex workers and LGBTQI individuals.

---

7 Konrad Adenauer Stiftung. (2021). Report on regulation of communication surveillance and access to internet in Africa.

8 Shirs, J., Hassib, B., et al. (2004). Gendered hate speech, data breach and state overreach.

External Evidence: The Human Rights Awareness and Promotion Forum (HRAPF) documents 9 evictions of LGBQTI individuals from rental properties in May 2025, linked to state crackdowns enabled by the AHA, 2023.[9] Coopamootoo et al. (cited in Shirs, J., Hassib, B., et al. 2004) highlight a "privacy gender gap," noting that women feel more vulnerable to online tracking but are less likely to adopt protective measures compared to men, a trend reflected in FGD reports of limited access to secure tools and trust of instant messaging apps.



9 Evictions of LGBQTI individuals from rental properties

Legal and Policy Gaps:

The 1995 Constitution (Article 27) prohibits interference with privacy; however, the Regulation of Interception of Communications Act (RICA), 2010, permits state interception for national security purposes, overseen by the Minister of Security and security officials, subject to court warrants. However, RICA is deficient in several areas:

- It lacks clear, objective criteria for courts to evaluate surveillance warrants, violating the principle of legality.
- It fails to ensure surveillance is necessary and proportionate, allowing arbitrary state actions.
- It omits post-surveillance notification, denying transparency to those monitored.
- It lacks an independent oversight body to regulate surveillance practices.

The AHA, 2023 (Sections 2(1), 2(3), 11), criminalises LGBQTI identities, enabling discriminatory state overreach and exacerbating digital coercion. The Data Protection and Privacy Act, 2019, provides a framework for protecting personal data, with Section 3 outlining principles of fair processing, purpose limitation, data minimisation, accuracy, limited retention, data subject rights, secure processing, and restricted international transfers.

However, its implementation is weak, and it lacks gender-specific protections against technology-facilitated abuses like phishing, revenge porn, and gendered disinformation. Tomiwa Ilori (2024) notes that Ugandan laws, including RICA, the Data Protection and Privacy Act 2019, and the Computer Misuse Act, 2011, fail to meet international privacy standards,[10] which require:

- **Legality:** Defined offences, targeted groups, time limits, due process, data storage safeguards, erasure protocols, and independent oversight.
- **Legitimacy:** Measures must serve the public interest, including public safety, crime prevention, public morals, rights protection, and national security.
- **Proportionality:** Judicial oversight and due process to prevent arbitrary state power.
- **Necessity:** Legitimate aims, user notification, and transparency.

These gaps enable arbitrary restrictions, disproportionately harming structurally silenced women through data breaches, digital coercion, and discriminatory enforcement, as confirmed by FGD reports of password demands and entrapment.

9 *Human Rights Awareness and Promotion Forum (HRAPF). (2025). Report on violence and violations based on real or presumed sexual orientation or gender identity during the month of May 2025.*

10 *Ilori, T. (n.d.). Framing a human rights approach to communication surveillance laws through the African human rights system in Nigeria, South Africa and Uganda.*

4. Policy Options

Option 1: Gender-Inclusive Legal Reforms

- Revise RICA to mandate clear, objective criteria for surveillance warrants, ensure necessity and proportionality, require post-surveillance notifications, and establish an independent oversight body. Amend the Data Protection and Privacy Act, 2019, to include gender-specific protections against technology-facilitated abuses. Repeal or revise discriminatory provisions in the AHA, 2023, to curb digital coercion and state overreach.
- **Pros:** Aligns with constitutional protections (Articles 21, 27) and international human rights standards; addresses systemic legal gaps to protect marginalised women.
- **Cons:** Faces resistance from state actors prioritising national security; legislative processes are slow and resource-intensive.
- **Example:** Amending RICA to require judicial oversight, as FGD participants demanded —"We need laws that stop the state from watching us without reason" — would enhance transparency.

Option 2: Strengthened Enforcement and Oversight

- Train law enforcement and regulators on gender-sensitive data protection practices to prevent digital entrapment and coercive tactics, such as password demands. Establish an independent, legislature-accountable oversight body to monitor surveillance compliance with legality, legitimacy, proportionality, and necessity principles.
- Pros: Promotes accountability; feasible through targeted training programs and oversight mechanisms.
- Cons: Requires political will and funding; patriarchal norms may hinder the enforcement of gender-sensitive policies.
- Example: Training police to respect privacy rights would reduce exploitation.

Option 3: Community Empowerment and Digital Safety Initiatives

- Implement WOUGNET-led digital literacy programs to educate WHRDs, structurally silenced communities, and women with disabilities on phishing prevention, secure communication, and data protection. Develop ethical guidelines for AI and biometrics to protect activists' anonymity during state crackdowns.
- Pros: Empowers marginalised women; fosters grassroots resilience and advocacy.
- Cons: Limited immediate impact on legal frameworks; resource-intensive for rural outreach and accessibility accommodations.
- Example: FGDs emphasised the need for digital literacy, with one participant stating, "We need to know how to spot phishing emails to stay safe," highlighting the demand for community-driven solutions.

Table: Comparison of Policy Options

Legal Reforms

Pros
Aligns with constitutional/international standards; systemic change

Cons
State resistance; slow process

Feasibility
Medium

Enforcement/Oversight

Pros
Promotes accountability; practical training

Cons
Needs funding; cultural barriers

Feasibility
High

Community Empowerment

Pros
Empowers women; grassroots impact

Cons
Limited legal change; resource-heavy

Feasibility
High

5. Recommended Policy Actions

FGDs with 25 structurally silenced women underscored the urgent need for targeted interventions to address pervasive fear, distrust, and digital exploitation. Their voices drive the following recommendations, clustered by stakeholder group for clarity and actionability:

To the Government of Uganda:

Legislative Reforms:

- **Amend RICA:** Require court warrants with clear, objective criteria, proportionality, and post-surveillance notifications to ensure transparency. Establish an independent oversight authority accountable to Parliament to monitor surveillance practices.
- **Revise the Data Protection and Privacy Act, 2019:** Incorporate gender-specific protections against technology-facilitated abuses, such as phishing, revenge porn, and gendered disinformation. Ensure compliance with principles like fair processing, data minimisation, secure storage, and restricted international transfers.
- **Repeal or Amend AHA, 2023:** Revise Sections 2(1), 2(3), and 11 to eliminate provisions enabling digital coercion and discrimination against LGBQTI communities (FGD: "Laws like AHA make us targets online and offline"). This would reduce state overreach, as evidenced by HRAPF's report of 9 LGBQTI evictions in May 2025.

Enforcement:

- Train law enforcement and regulators on gender-sensitive practices to prevent digital entrapment and coercive tactics, including the demand for passwords. This includes workshops on respecting privacy rights and recognising the gendered impacts of surveillance, addressing FGD reports of police exploitation.
- Develop a national enforcement framework to ensure compliance with the Data Protection Act, incorporating regular audits to prevent unauthorised access to data by state actors.

To Civil Society (e.g., WOUGNET, HRAPF):

- **Digital Literacy Programs:** Launch comprehensive awareness campaigns on data protection and privacy rights for WHRDs, sex workers, marginalised communities, and women with disabilities. Focus on phishing prevention, secure communication, and encryption tools (FGD: "We need to know how to spot phishing emails to stay safe"). Programs should include practical training on identifying malicious links and securing devices, addressing the FGD-reported hacking incidents.
- **Advocacy:** Mobilise grassroots campaigns to pressure the government for legal reforms and oversight, amplifying FGD voices (e.g., "I stopped posting because I fear being tracked"). Partner with organisations like HRAPF to advocate for AHA amendments, using the 9 eviction cases as evidence of harm.
- **Accessibility:** Ensure digital safety workshops are inclusive, providing sign language, braille, and accessible digital tools for women with disabilities. Collaborate with disability rights groups to tailor programs to their needs.
- **Community Engagement:** Establish peer-support networks for structurally silenced women to share strategies for digital safety, building on FGD insights about distrust and fear.

To the Private Sector (e.g., Telecommunications Companies):

- **Ethical Practices:** Cease complicity in communication surveillance by adopting transparent data protection policies and refusing unauthorised data sharing with state actors. Implement internal audits to ensure compliance with the Data Protection Act.
- **Support Digital Safety:** Partner with civil society to provide encryption tools, anonymity software, and secure communication platforms for structurally silenced women. Fund digital literacy initiatives to address the FGD-reported lack of awareness of phishing and other forms of malicious intrusions.
- **Corporate Accountability:** Publish annual transparency reports detailing government data requests, empowering women to trust telecom services, as FGDs highlighted distrust in telecommunications companies.

To Specific Agencies (e.g., UCC, NITA-U, MoICT&NG):

- **Ethical AI and Biometrics Guidelines:** Develop frameworks to ensure AI and biometric technologies protect activists' anonymity during state crackdowns (FGD: "AI tracking scares us; we need ways to stay anonymous"). Guidelines should prioritise consent, data minimisation, and secure storage, addressing concerns about invasive technologies raised during FGDs.
- **Regulatory Oversight:** Enforce compliance with the Data Protection Act, 2019, by monitoring telecommunications companies and imposing penalties for unauthorised data sharing. Establish a reporting mechanism for women to flag privacy violations, addressing concerns raised by FGDs about telecom company complicity.
- **Technology Development:** Support the creation of accessible, women-friendly digital tools, such as apps with disability-compatible interfaces, to address concerns about inaccessibility raised by FGD.

Justification:

- FGDs highlight a pervasive climate of fear, self-censorship, and digital exploitation (e.g., "Every call feels like a trap"; "Fake profiles trick us"), necessitating urgent legal, enforcement, and community interventions.
- Legal reforms align with constitutional protections (Articles 21, 27) and international standards (Tomiwa Ilori, 2024; UN Special Rapporteur), addressing systemic gaps.
- Community empowerment tackles the privacy gender gap, equipping women with tools and knowledge to navigate digital risks, as emphasised in FGDs.

6. Implementation Considerations

Action Steps:

- Multi-Stakeholder Task Force: Form a collaborative task force including government representatives, WOUGNET, HRAPF, telecommunications companies, and the Uganda Communications Commission to review and propose specific amendments to RICA, the Data Protection Act, and AHA. The task force should integrate FGD insights, such as demands for transparent surveillance laws, to ensure women's voices shape reforms.
- Pilot Digital Literacy Workshops: Launch WOUGNET-led workshops in urban and rural areas, training women on phishing prevention, encryption, and secure communication. Ensure accessibility with sign language, braille, and disability-friendly tools.
- Funding and Partnerships: Secure funding from international partners like the Association for Progressive Communications (APC) and UN agencies to support training, oversight mechanisms, and digital safety tools. Partner with disability rights organisations to enhance accessibility.

Challenges:

- State Resistance: Government prioritisation of national security and patriarchal norms may hinder legal reforms, particularly for AHA amendments.
- Resource Constraints: Limited funding for rural outreach and accessibility accommodations.
- Political Sensitivity: AHA reforms face resistance due to cultural and political opposition to LGBTQ rights, as evidenced by HRAPF's eviction data.
- Private Sector Reluctance: Telecommunications companies may resist transparency due to state pressure, as noted in FGDs about telecom complicity.

Mitigation Strategies:

- **Stakeholder Consensus:** Leverage WOUGNET's validation workshop to build consensus by presenting FGD findings and aligning stakeholders on reform goals.
- **NGO Partnerships:** Collaborate with NGOs to secure funding and expertise, ensuring rural outreach and accessibility tools, such as braille and sign language interpreters.
- **Framing Reforms:** Position legal and enforcement reforms as enhancing public safety and national security to gain government buy-in, addressing FGD fears of arbitrary surveillance.
- **Private Sector Incentives:** Offer incentives, such as public recognition, to telecoms that adopt transparent data policies, countering FGD distrust in telecommunications.

7. Conclusion

Structurally silenced women in Uganda face a hostile digital environment, with FGDs from 25 women WHRDs, women with disabilities, sex workers, and LGBQTI individuals revealing pervasive fear, distrust, and exploitation through surveillance, data breaches, and digital coercion. Statements like “I can’t trust my phone and shadow; every call feels like a trap” and “Fake profiles trick us into sharing messages” underscore the chilling effect on digital activism. Legal gaps in RICA, the Data Protection and Privacy Act, 2019, and the AHA, 2023, exacerbate these violations, thereby undermining constitutional protections (Articles 21 and 27). A multifaceted approach, combining gender-inclusive legal reforms, robust enforcement, and community empowerment, addresses these challenges, empowering marginalised women to navigate digital spaces safely. With the 2026 elections approaching, the government, civil society, private sector, and regulatory agencies must act swiftly to implement targeted recommendations, ensuring digital safety and equality. By amplifying the voices of the 25 women, this brief calls for urgent collaboration to uphold Uganda’s constitutional commitments and international human rights standards, fostering an inclusive digital future.

“I can’t trust my phone and shadow; every call feels like a trap” and “Fake profiles trick us into sharing messages”

8. Reference List

Constitution of Uganda, *1995 (Articles 21, 27).*

Regulation of Interception of Communications Act, *2010.*

Data Protection and Privacy Act, *2019 (Section 3).*

Anti-Homosexuality Act, *2023 (Sections 2(1), 2(3), 11).*

UN Special Rapporteur on Freedom of Expression, *Report on Communication Surveillance.*

Women of Uganda Network (WOUGNET), *FGD Findings with 15 Structurally Silenced Women, 2025.*

Women of Uganda Network (WOUGNET)
P.O Box 138387, Kampala, Uganda
Tel: +256 394 823109 / +256 414532035
Toll Free: 0800200510
Email: info@wougnet.org

www.wougnet.org