# SECOND GLOBAL SYMPOSIUM ON TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE: KEY TAKEAWAYS

**"The path ahead is indeed challenging. Yet it is the collective expertise, resilience and determination of forums like this Symposium that fuel our optimism and drive for change. I urge everyone here – policymakers, tech-industry leaders, activists and engaged citizens – to unite in our fight against technology-facilitated gender-based violence. The journey towards a safer digital environment is a shared responsibility, and one that we undertake not just for ourselves, but for future generations."**

**Hon. Lynda Tabuya, Minister of Women, Children and Social Protection, Fiji**

## INTRODUCTION

In February 2024, UNFPA, the United Nations sexual and reproductive health agency, in partnership with Australia's eSafety Commissioner, hosted the Second Global Symposium on Technology-facilitated Gender-based Violence (TFGBV). This forum included 44 speakers, representing 27 different countries, and between 400 and 800 participants each day from diverse technical and geographical backgrounds.

The Symposium took place virtually across three days, to track progress and exchange promising best practice in addressing TFGBV. It also served as a platform for consultations regarding UNFPA's Framework for TFGBV Programming, developed in partnership with Australia's eSafety Commissioner and on behalf of the Global Partnership for Action Against Gender-based Online Harassment and Abuse.

**This brief highlights key insights and recommendations identified during the Symposium.**

UNFPA

making all spaces safe.

# EMERGING RISKS OF TECHNOLOGY

The recent and rapid evolution of technology has introduced new tools and platforms that, while beneficial, have also expanded opportunities for abuse and exploitation. Broadly speaking, these technologies are:

- **Generative artificial intelligence (AI):** The proliferation of generative AI tools to create synthetic content has amplified TFGBV. Synthetic content can be used for disinformation, impersonation, and image-based abuse, creating new challenges for detection and accountability. The increased reliance on AI also amplifies gendered bias in the everyday lives of women and girls in all their diversity.
- **Virtual reality (VR):** VR introduces unique risks including a mask of anonymity that allows perpetrators to hide their identities; immersive environments that intensify the psychological impact of violence; and the extensive collection of biometric data without users' knowledge or consent. Data extracted from facial recognition, voiceprints and body movements can be exploited for the stalking, blackmail or surveillance of women and girls.
- **Internet of Things:** The increasing interconnectedness of devices, such as smart cameras, home assistants, home security systems and location trackers, can create new avenues for perpetrators to surveil and control individuals or groups. The high accessibility and affordability of these devices has led to increasing misuse.

**"Technology has become integrated into our everyday lives, and the more affordable and accessible tools become, the more they will be misused and woven throughout tactics of abuse."**

**Erica Olsen, Safety Net Project Director, National Network to End Domestic Violence, United States of America**

# BUSINESS MODELS FOR TECHNOLOGY

Business models for technology can contribute to the proliferation of TFGBV through the following:

- **Engagement-driven algorithms:** Many algorithms prioritize user-engagement metrics – such as interaction rates and time spent on platforms – over quality and safety, allowing harmful content to proliferate. At the same time, malicious and misogynistic content is amplified by algorithms due to its provocative and "clickbait" nature, thereby generating high levels of engagement and spread.
- **Lack of transparency:** Technology companies often lack transparency in how their algorithms and data collection systems operate. Users may be unaware of how their personal information is collected, shared and used, and hold little control over opting out of sharing their data.
- **Opaque data markets:** Technology companies profit from the sale of personal data through opaque and often unregulated data markets, enabling the targeted dissemination of harmful advertisements and content for users.
- **Capacity gaps:** Technology teams are often gender blind, and as such, lack an understanding of how their products may be misused to perpetrate TFGBV. Similarly, individuals and organizations working to promote the rights of women and girls require increased investment in their digital literacy, in order to protect their own safety, privacy and security as well as that of their clientele.

Exploitative business models that are driven by profit and which lack transparency are currently the norm. However, there are some areas of work which can facilitate reform. These include:

- **Funding independent research:** Introducing levies or licensing fees for technology companies to support independent research on improving the safety, security and privacy of women in all their diversity can be a key strategy in preventing and mitigating TFGBV.
- **Advancing the role of women in science, technology, engineering and maths:** Increasing women's participation in the tech industry by improving access to employment, leadership opportunities and capacity-building programmes can support the integration of gender-centred ideation, design and development of technology.
- **Regulating data collection and use:** Establishing stricter regulatory frameworks, including an "opt out" option for data collection as the default for tech products, can ensure transparency in how user data is collected, stored and utilized. In addition, mandatory disclosures and compliance with ethical data practices can prevent misuse and protect vulnerable groups from targeted harm.
- **Improving market transparency:** Policies that require tech companies and data brokers to disclose their data-sharing practices, partnerships and business models could promote more ethical behaviour by corporations with regards to the monetization of user data.

# RESPONDING TO TFGBV

Responding to TFGBV is challenging for a number of reasons, including:

- **The online–offline continuum of violence:** TFGBV is not an isolated experience, but exists across a continuum where online violence can intersect with, escalate, or mirror offline violence and vice versa. This continuum can complicate response efforts as interventions must address both digital and physical safety, requiring coordinated, multi-sectoral approaches.
- **Inadequate complaint mechanisms:** Organizations responding to TFGBV often face challenges when working with tech companies that do not have sufficient mechanisms or staff to ensure effective and timely responses. Tech companies may also be inconsistent in responding to complaints or addressing product design flaws that facilitate TFGBV with little recourse or accountability to survivors.

**"Helplines run by institutions often view technology as apolitical and neutral, so they don't have a gender and intersectional perspective in the way they approach and analyse digital risk. On the other hand, helplines that are set up by civil society and specialize in supporting human rights defenders and activists don't always have sufficient skills or experience in supporting people that are facing gender-based violence and hate speech in digital spaces.**

**These two gaps result in an international landscape that lacks awareness on how to address risks faced by women and populations traditionally discriminated against. This is a concern because those groups are disproportionately exposed to gender-based violence. In order to overcome those gaps, civil society organizations, especially small feminist collectives, organize themselves to create networks of information, support and solidarity, and initiatives, services and resources to break the sense of isolation, guilt or shame that is experienced by survivors so they can heal and recover."**

**Alexandra Haché, Digital Defenders Partnership**

Effective responses to TFGBV require integration with broader gender-based violence (GBV) programmes, coordination mechanisms and policies. Actions that ensure survivor-centred responses include:

- **Integrating TFGBV into the wider infrastructure of GBV programming:** Specialized training and job aids can equip those who provide services to people affected by GBV with the knowledge and skills required to address TFGBV effectively. Partnerships with non-traditional GBV actors, including tech companies and feminist technologists, are critical for supporting effective responses.

- **Responding to individual survivor needs:** Effective responses to TFGBV should be survivor centred and comprehensive, and include the following:

  - GBV case managers' **access to expert TFGBV support** when required, in order to comprehensively assess a problem in consultation with survivors of TFGBV.

  - **Robust referral** to local authorities, law enforcement bodies, legal services and healthcare providers (including for mental health), as well as tech platforms when managing survivors' online complaints.

  - Provision of **safe accommodation** for survivors, including cash assistance.

  - In-depth **tech safety assessments** for survivors (and their children) to address immediate safety concerns and develop a safety plan to mitigate further harm, including the provision of alternative methods for safe communication, such as burner phones and a safe email account.

  - Provision of **accessible guidance** and resources to survivors, to ensure their immediate and long-term safety as well as to mitigate further occurrences of TFGBV.

  - **Increased capacity building** for frontline providers so that they can respond in a timely and effective manner to the needs of survivors of GBV.

- **Helplines for survivors of TFGBV:** Helplines that are led by, or are in coordination with, existing GBV programmes and are grounded in feminist methodologies to address gaps in trusted, survivor-centred support, should be established or strengthened. These hotlines should prioritize local context, provide digital literacy resources, and raise awareness of legal rights.

- **Adapt referral pathways:** New partners should be integrated into case management systems to support the referral of survivors to appropriate services, including psychological support, legal assistance and specialized resources for responding to TFGBV.

- **Enhance content moderation:** Robust escalation pathways for content moderation should be established, and supported by context-specific, human-led reviews to effectively address cases of TFGBV effectively.

**"What's really critical is that we understand what the survivors' priorities are… we're led by what the survivor needs, and then we create a safety plan with their consent so that they feel empowered. [This includes] helping navigate settings [and] other tech features. We look for evidence of a perpetrator monitoring them, and use technology to create evidence that the perpetrator has had access to their accounts and devices. The survivor can then present this to the police."**

**Emma Pickering, Refuge**

# PREVENTING AND MITIGATING TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE

Preventing TFGBV is challenging for a range of reasons, including the complex and unregulated systems of data generation and use, constantly evolving technologies and low levels of digital literacy. Other challenges include:

- **Negligent tech design:** Many technologies, even those that are well-intentioned, are created without considering the potential for them to be used to perpetrate TFGBV.
- **Limited resources to ensure contextualized programmes:** Effective prevention of TFGBV requires a deep, localized understanding of target communities as well as of participatory design processes. Without adequate resources to contextualize programmes, interventions can overlook cultural, legal or digital literacy factors critical to preventing TFGBV.
- **Reaching and engaging young people:** Young people are digital natives who engage with rapidly evolving technologies often beyond the reach of traditional prevention programmes. Young people's swift adoption and use of new platforms, tools and products exposes them to greater risks, making them one of the most vulnerable yet hardest-to-reach groups in efforts to prevent TFGBV.

**"Social and cultural differences in regions need to be taken into account when developing policies that regulate AI-facilitated gender-based violence."**

**Nighat Dad, Digital Rights Foundation**

To address the unique challenges and risks associated with TFGBV, prevention programmes should include community-based, institutional and technological interventions that take into account the following:

- **Ethical design of technology:** Tech teams must incorporate the following into the design of their products and services:
  - **"Do no harm"**, including carrying out risk assessments, weighing risks against potential benefits, safely testing products, and considering impact on a diverse category of users with particular consideration to the risks of TFGBV.
  - **A participatory approach** that includes diverse voices, particularly those of survivors and the service providers that support them, specialists in gender and human rights, and historically marginalized groups (e.g. women, girls, gender-diverse communities, people with disabilities).
  - **Guaranteed privacy, choice and intuitive tech,** so that users can actively make informed decisions about their privacy settings by easily navigating configuration settings facilitated by neutral and simple language.
  - **Strengthened security and data,** by considering how technology may be misused and developing sophisticated models that include context-specific risks for TFGBV.
- **Challenging and reforming the tech business model:** Business models and data practices should be adapted to prioritize safety and ensure systems of accountability and reparation. This could include a "technology trust mark" system that assesses and rates social media platforms' adherence to safety standards; training on TFGBV for tech product designers and developers, so that safety-by-design is integrated from ideation through to implementation; and regulating data generation and use.

- **Promotion of ongoing public education and digital literacy:** Investment in the incorporation of digital literacy into community education programmes should be increased. Educational topics may include how to stay safe online; practical security measures individuals can take, including how to use privacy settings, two-factor authentication, and platform complaint mechanisms; respecting others online and maintaining healthy relationships; legal rights and remedies that exist in a particular context; and where to go for help, including available psychosocial and legal services.
- **Community-based approaches:** Prevention programmes should be adapted to local contexts; this requires co-creation and implementation alongside community stakeholders.
- **Education and digital literacy:** Digital literacy should be incorporated into educational programmes, such as comprehensive sexuality education or community-based programmes, to empower users in navigating technology safely.

**"TFGBV is not just about perpetrators; it reflects the complex interplay between geopolitics and technology, and this requires proactive engagement to address vulnerabilities up and down the stack from Big Tech to big finance and everything in between. And this is how we hold them to account. Wrapping up safety by design is another way we're working with industry to reduce the threat surface. And this is crucial because it ensures that platforms are understanding and assessing the risks and harm, and prioritizing safety from the outset, building it in rather than bolting it on after the harm has been done."**

**Julie Inman-Grant, eSafety Commissioner, Australia**

# LEGISLATIVE AND REGULATORY REFORM

Legislative and regulatory frameworks can create an enabling environment where perpetrators are held accountable, survivors can access justice, and technology companies are incentivized to prioritize safety. Existing challenges to creating an effective regulatory response include:

- **Evolving technologies:** Existing legal frameworks often fail to keep pace with the rapidly evolving nature of technology and its misuse.
- **Fragmentation across jurisdictions:** A lack of consistent definitions and approaches to TFGBV across jurisdictions complicates enforcement and cross-border cooperation.
- **Unintended consequences:** Cybercrime legislation, for example, while aimed at addressing TFGBV can sometimes have adverse impacts, such as curbing freedom of expression or disproportionately affecting marginalized groups.
- **Enforceability:** The use of regulation to enforce safety-, security-, and privacy-by-design, and ensuring accountability to prevent harm and promote effective response mechanisms, is limited.

**"The impacts of poor legislation or legislation without a gender and human rights perspective can be devastating. This is particularly significant given the dual nature of digital technologies and the Internet: they can serve as spaces where violence occurs but also as platforms for accessing vital information, including how to protect yourself from TFGBV and collectively organizing to defend gender equality"**

**Jamila Venturini, Co-Executive Director, Derechos Digitales**

New industry standards and rights-based law reform are required to support a robust regulatory environment to address TFGBV. These include:

- **Rights-based law reform:** Intersectional, evidence-based legislation and policy should be developed through participatory cycles to ensure that it prioritizes survivor protection as well as the accountability of perpetrators, including tech companies. Transparency of data economies, and brokers in particular, should be legislated to mitigate TFGBV and protect the safety, security and privacy of users. Laws and policies should be developed in concert with the existing regulatory framework to minimize confusion, ambiguity and opportunities for the perpetration of TFGBV.

- **Participatory policy development:** Public policy and legislation should be developed through inclusive, participatory approaches, consulting diverse stakeholders such as civil society organizations and experts to create rights-based, trauma-informed, localized and adaptable solutions for effectively addressing TFGBV.

- **Industry standards and best practices:** Global industry standards, such as those developed by the Digital Trust & Safety Partnership should be advocated for and adopted. These include:

  - Embedding safety-by-design principles in product development.
  - Establishing governance mechanisms and trust and safety teams.
  - Enhancing transparency through accountability initiatives that demonstrate how safety standards are implemented.

- **Auditing and transparency of tech companies:** Independent audits should be mandated and transparency obligations enforced for technology companies. This should include the disclosure of algorithms, training datasets, inputs to identify biases and potential harms, and data collection, storing and sharing practices.

- **User safety tools:** Platforms should be required to publicize user safety tools in multiple languages, and educate users on their technology to facilitate informed digital engagement.

**"If we want to build legislation that is sensitive to context, that responds to the actual needs and realities of survivors in their supporting groups, we need to include different stakeholders involved in combating TFGBV in policy and regulatory discussions."**

**Jasminka Džumhur, Human Rights Ombudsperson of Bosnia and Herzegovina**

# OVERALL RECOMMENDATIONS

- **Adopt an evidence-based, participatory approach:** Strategies and programmes to address TFGBV are best informed by a strong evidence base, including a comprehensive and localized participatory needs assessment that engages women, girls and survivors in target communities and the professionals that work with them.

- **Respond to the local context:** Despite its universality, TFGBV is highly contextual. This means that survivors' experiences are influenced by the social and gender norms of their communities as well as their language, digital literacy and access to technology. Understanding local context is critical in identifying the specific manifestations and impacts of TFGBV in order to design programmes and policies that are responsive to the needs of survivors.

- **Build multi-stakeholder partnerships:** Addressing TFGBV requires an interdisciplinary and multisectoral approach. Prevention and response programmes, technology products, global governance frameworks, and regional and national laws, policies and strategies must involve a diversity of stakeholders in their design and implementation.

- **Create safety-, security- and privacy-by-design:** To effectively prevent and mitigate TFGBV, tech companies and platforms must embed safety, security and privacy considerations into every stage of tool development – from conception and design to deployment and maintenance. This includes an approach to AI development that integrates intersectional feminist principles at its core, and which can serve as a potent tool to prevent or mitigate TFGBV.

**"We are all speaking different languages. For example, the gender-based violence sector has a common language around gender-based violence principles, and trauma-informed and survivor-centred care [but other] actors from different sectors are joining this space who have never been exposed to this language [in the same way that] gender-based violence actors have not been exposed to language around tech. This leads to issues and responses being understood very differently."**

Participant in break-out session Day 2, Group 3, Second Global Symposium on Technology-facilitated Gender-based Violence

# ACKNOWLEDGEMENTS

Special thanks go to the speakers who shared their insights with us at the Second Global Symposium on Technology-facilitated Gender-based Violence. These are (in order of appearance):

**Julitta Onabanjo**, Director of Technical Division, UNFPA
**Alexandra Robinson**, Gender-based Violence Technical Advisor, UNFPA
**Mariam Jobe**, Africa Internet Governance Forum Secretariat
**Jan Moolman**, Co-Cartographer/Co-Executive Director, Numun Fund
**Shermeen Sarbast**, Project Manager, Arabi Facts Hub
**Nighat Dad**, Executive Director, Digital Rights Foundation
**Leonie Tanczer**, Associate Professor, University College London
**Kavya Pearlman**, Founder and CEO, X Reality Safety Intelligence
**Erica Olsen**, Safety Net Project Director, National Network to End Domestic Violence, the United States of America
**Amanda Manyame**, Digital Rights Advisor, Equality Now
**Marwa Fatafta**, MENA Policy Manager, Access Now
**Rachel Magege**, Lawyer and Data Governance Lead, Pollicy
**Lucy Purdon**, Director, Courage Everywhere
**Maha Jouini**, AI Country Researcher, Global Index on Responsible AI
**Abdul Hakeem Ajijola**, Member, African Union Cybersecurity Experts Group
**Varina Winder**, Chief of Staff, Secretary's Office of Global Women's Issues, Department of State, the United States of America
**Hon. Lynda Tabuya**, Minister of Women, Children and Social Protection, Fiji
**Hera Hussain**, Founder and CEO, Chayn
**Emma Pickering**, Head of Tech and Economic Abuse, Refuge
**Sherri Talabany**, President and Executive Director, SEED
**Vaela Devesi**, Director for the Women's Development Division, Ministry of Women, Youth, Children and Family Affairs, Solomon Islands
**Alexandra Haché**, Community Building Officer, Digital Defenders Partnership
**Hyra Basit**, Cyber Harassment Helpline Lead, Digital Rights Foundation
**Hanneke Kastelijns**, Programme Manager, Tech for Peace
**Ella Serry**, Manager of International Engagement, eSafety Commissioner, Australia
**Devina S**, Technology-facilitated Gender-based Violence Consultant, UNFPA
**Leisha Beardmore**, Senior Gender-based Violence Advisor, Save the Children
**Emma Fulu**, Founder and Executive Director, Equality Institute
**Julie Inman-Grant**, eSafety Commissioner, Australia
**Cherie Oyier**, Programmes Officer for Women's Digital Rights, Kictanet
**Eva Galperin**, Director of Cybersecurity, Electronic Frontier Foundation
**Emily Springer** PhD, Consultant, TechnoSocio Advisory LLC
**Candela Yatche**, Founder and Director, Bellamente
**Toby Shulruff**, Principal Consultant, Toby A. Shulruff Consulting
**Jameela Sahiba**, Senior Programme Manager for Emerging Technologies, The Dialogue
**Chinmayi SK**, Founder, Bachchao Project
**Jamila Venturini**, Co-Executive Director, Derechos Digitales
**Farzaneh Badiei**, Head of Outreach and Engagement, Digital Trust & Safety Partnership
**Michelle Bordachar**, Legal and Legislative Advisor of the National Cybersecurity Coordination, Ministry of the Interior and Public Security
**Eduardo Carrillo**, Co-Executive Director, Tedic
**Jasminka Džumhur**, Human Rights Ombudsperson of Bosnia and Herzegovina
**Sharon Armstrong**, Director General for the Social Development Bureau, Global Affairs Canada

MARCH 2025

UNITED NATIONS POPULATION FUND

605 THIRD AVENUE NEW YORK, NY 10158

TEL. +1 212 297 5000

WWW.UNFPA.ORG