2022 Global Symposium on Technology-facilitated Gender-based Violence Results: Building a Common Pathway

Acknowledgements

Contents

Executive summary

The United Nations Population Fund (UNFPA) and the Wilson Center's Science and Technology Innovation Program held a three-day expert symposium on technology-facilitated gender-based violence (TF GBV) with stakeholders from civil society, academia, the technology industry, government, regulation, and intergovernmental organizations and representatives from every continent, including over 25 countries.

The purpose of the symposium was to: (1) provide a platform for exchanging knowledge and good practices by civil society organizations and technology companies to address TF GBV; (2) identify challenges and opportunities to advance progress; and (3) foster collaboration and partnerships between actors in the TF GBV space, to create innovative solutions that comprehensively address the issue.

This report consolidates the discussions and key areas of agreement discerned during the three-day global symposium. It has been structured thematically and chronologically, following the experiences and discussions that arose in each of the three selected focus areas. Each day included panel presentations followed by expert breakout sessions across three major themes and discussion topics:

1. **Data and measurement, methodology matters:** The first day focused on ethical data principles and practices currently being used across intersecting fields and how they are applied or could be applied to TF GBV. Topics explored included data quality, intersectionality, survivor-centred approaches, ethics, safety and security. Breakout sessions addressed information needs, data-collection methods and practices, data storage and management, data analysis, data ownership and dissemination.

2. **Business and technology, feminist Internet:** The second day focused on feminist design frameworks and practices across various areas of expertise and discussed how they can be applied to prevent and respond to TF GBV. Topics centred on exploring Safety/Privacy/Security by Design, artificial intelligence bias, trauma-informed computing and the default male-centred technology design. Breakout sessions covered entry points for Safety by Design, adopting a feminist design framework in industry standards, default survivor-centred approaches, community of practice and Global North–South equity.

3. **Law and policy, rights-based regulation:** The last day focused on laws, policies, challenges and rights-based approaches to TF GBV in different contexts. Discussions included issues of self-regulation, national regulation, encryption, survivor-centred policy and future-proofing. Breakout sessions discussed models and processes, backdoor encryption, unintended consequences, overcoming challenges and accountability.

Below are key takeaways from each of the above mentioned themes. A detailed breakdown of all topics, discussions and outcomes, including quotes from participants, around each can be found within the associated sections of this report.

Data and measurement key takeaways

- TF GBV data practices must, as a minimum, be grounded by global GBV data ethics but then be further expanded upon, given that digital collection, use and management of digital data bring even higher risk than purely analogue.

- Caution should be used with TF GBV data practices to avoid replicating extractive data-collection practices, common within the technology industry.

- Risk of harm to survivors should always be given more importance than any potential benefit for data and research. TF GBV data collection should not occur unless participants' safety is ensured; specifically, TF GBV response services must be established.

- The understanding of data ownership must shift from something that can be indefinitely owned by a company, organization or government to something that is an extension of the human, requiring fully informed and ongoing consent for its storage and use.

- Consent must be an authentic and ongoing interaction, not a one-off exercise.

- Unethical generation, management and misuse of data may lead to TF GBV, including data collection on TF GBV specifically.

- More evidence is needed on TF GBV, especially in low- and middle-income contexts and in humanitarian settings.

- Do no harm, survivor-centred, intersectional and participatory research processes must be considered across all steps of the research/ data process: from defining needs to data collection, analysis and dissemination.

Business and technology key takeaways

The needs of survivors must be understood and incorporated throughout the product lifecycle through participatory processes in the design, deployment and management of technology products, processes and systems. Ethical and safety standards for GBV data recommend against directly interviewing or collecting data from known survivors unless minimum standards are met and in place.[1]

- Power imbalances must be identified and countered.

- A holistic assessment and shift of business status quo is necessary for women to be safe, including core functions, business models and operations of technology.

- Innovative approaches and ideas, grounded in offline GBV normative frameworks and expertise, are necessary to ensure the proper safety of women and girls in the digital age.

- Industry standards must be grounded in global experiences and intersectional perspectives to support the technology industry and be more easily regulated for safety.

- Safety by Design, survivor-centred and intersectional approaches in technology development must be enforced from the beginning, and integrated and normalized throughout tech companies' processes.

- Multidisciplinary teams are best positioned to address TF GBV holistically. Partnerships and collaborations across sectors are central to properly understanding and creating effective solutions.

- Context is crucial to understanding, preventing and effectively responding to TF GBV globally.

---

1 Best practice is to interview and collect data from women, knowing that one in three women has experienced GBV in their lifetime. Treat every woman as a survivor, but do not ask specifically if they have been subject to GBV. This information is often not necessary and immediately increases risk of harm to everyone involved.

- Survivor-centred and trauma-informed technology to respond to TF GBV and offline GBV can be developed ethically, and examples of good practices exist.

Laws and policies key takeaways

- Approaches and beliefs differ around freedom of expression, privacy and criminalization; therefore, human-centred and survivor-centred approaches and perspectives are necessary to ensure policy and regulation are not doing more harm.

- A combination of self-imposed policy by technology companies, government regulation, community regulation, as well as global and regional frameworks and partnerships, are necessary to prevent and end TF GBV globally.

- Centring on human rights within policy rather than on specific acts or definitions of TF GBV minimizes the weaponization of regulation against activists and is more future-proof.

- Alternative solutions, such as metadata, should be explored in place of backdoor encryption. The existence of encryption keys or tools create opportunities for bad actors to attack users risks to survivor safety outweigh the potential benefit.

- Context matters – human rights-based and survivor-centred approaches are necessary to ensure regulation is not weaponized against survivors or activists and does not violate privacy or freedom of speech.

- The problem must be recentred on what survivors need rather than on what policymakers think women and girls need or what is convenient to implement.

- Increased digital literacy is necessary for policymakers and regulators to address TF GBV, particularly in emerging technologies.

- Laws and policies must be developed in partnership with survivor advocate organizations, feminist technologists and lawyers groups.

- Global and cross-border regulations and partnerships are needed while accounting for contextual and cultural specificities that reflect the experiences of TF GBV and help-seeking behaviours.

Background

UNFPA Guatemala / Tracie Méndez

Humanity is in the midst of a digital revolution. Technological innovation and digitalization in all parts of the world have significantly accelerated in the past few years, representing a critical opportunity for sustainable development. Technology has the potential to foster economic growth, expand access to education and evidence-based information and knowledge, enable access to life-saving services, including health care, and enhance participation in public and political life and democratic processes. It does so by giving voice and power to those who have traditionally been left behind (UNFPA, 2021a).

Technology and digital spaces provide extensive opportunities through their contribution to women's empowerment and ending gender inequalities. However, technology products and platforms are also spaces and tools which can be wielded, either with or without intention, to cause harm. They enable gender-based violence to be committed, assisted, aggravated and amplified. Technology-facilitated gender-based violence (TF GBV) targets all women but is particularly pervasive among those women and girls with intersecting identities (Dunn et al., 2023; UNFPA, 2021a). Further, women who use

technology and digital spaces in their professional lives, such as journalists, activists and politicians, are disproportionately targeted with TF GBV. This has a detrimental silencing effect and serious consequences for democracies and societies (UNFPA, 2021a).

> **The United Nations Population Fund (UNFPA) has defined technology-facilitated GBV as: any act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media, against a person on the basis of their gender (UNFPA, 2021a).**

TF GBV is widespread. Available data from 51 countries with the highest Internet penetration rates suggest that as many as 38 per cent of women have personally experienced online violence, while 85 per cent of women have witnessed online violence being committed against another woman (The Economist Intelligence Unit, 2021). Over half, or 58 per cent of all young women and girls, between 15 and 25 years of age, have been subjected to online harassment in 22 countries globally (Plan International, 2020). These

statistics show that TF GBV is not only shockingly pervasive but starts early and contributes to the normalization of GBV against women and girls online and offline.

TF GBV shares common characteristics with other forms of GBV, such as its presence in all societies worldwide, its gendered nature and roots in gender inequality, and its disproportionate and severe impact on the lives of women and girls. Additionally, TF GBV has specific characteristics related to its digital nature: anonymity, action at a distance, accessibility, affordability, automation, collectivity, impunity, normalization of violence, perpetuity and propagation. These characteristics stem from the design and mode of functioning of technology and digital platforms. Abuse is amplified by artificial intelligence (AI) algorithms that seek maximum user engagement and contribute to the normalization of violence. This makes TF GBV particularly challenging to address with existing GBV response systems and mechanisms, highlighting the need for multidisciplinary action and collaboration (UNFPA, 2021a).

Furthermore, TF GBV often occurs in a continuum of online and offline violence. In a context of offline violence, abuse is likely to continue in online spaces and through technological means, and vice versa: abuse that starts in the digital world can turn into threats and actions of physical violence (UNFPA, 2021a). For example, in cases of intimate partner violence, survivors are stalked and surveilled by violent and abusive partners using technology tools. Conversely, instances of online violence, threats and hate speech against women in public may encourage sexual or physical violence towards women and even lead to femicide.

Addressing TF GBV is no longer negotiable. Technology and digital spaces should serve as tools to accelerate the achievement of gender equality rather than tools for subjugation, reinforcement of harmful gender norms and stereotypes, perpetuation of violence, and silencing of women and girls in all their diversity

(UNFPA, 2021a). TF GBV is a global problem that requires globally coordinated solutions. Thus, while the impact and manifestations of TF GBV are highly contextual – siloed national and sectoral approaches cannot solve the issue. The Global Partnership for Action on Gender-Based Online Harassment and Abuse (the Global Partnership) is one such effort for coordinated and interdisciplinary action to address TF GBV. Launched in 2022 by the governments of the United States of America and the Kingdom of Denmark, the Global Partnership is now a 12-country coalition. It is working alongside a multi-sectoral advisory group that brings evidence-based and coordinated solutions, principles and policies to address the issue of TF GBV. Its objectives include developing and advancing shared principles, increasing targeted programming and resources, and expanding access to reliable, comparable data (Office of the Spokesperson, 2022).

The multidisciplinary nature of the issue means that silos persist. Silos persist where women, civil society and non-governmental organizations (NGOs) are not included in the technology design process from the onset. They persist when tech companies do not enforce Safety by Design in partnership with these experts. They persist among GBV practitioners, who need to be more digitally literate to communicate the specific needs of survivors or the risks of harm and need more tools to provide immediate and effective responses to incidences of TF GBV. They persist among legislators unfamiliar with technology and therefore unable to develop effective laws and policies.

To address TF GBV, intersectional and multidisciplinary expertise, learning and collaboration is crucial. The Global Symposium on Technology-facilitated Gender-based Violence held in late 2022 was one of the first global convening efforts to progress collective action from a global and interdisciplinary perspective. Its aim to break down silos and work towards creating a common language to enable collective action was achieved.

About the Conveners:
the United Nations Population Fund (UNFPA) and the Wilson Center

UNFPA, the UN sexual and reproductive health agency, is working to achieve three transformative results by 2030: to end the unmet need for family planning, to end preventable maternal deaths, and to end GBV and harmful practices. UNFPA recognizes that ending GBV means ending violence in all spaces, including online and technology (UNFPA, 2021a). TF GBV is therefore a critical area of concern for UNFPA, as acknowledged in the 2022–2025 UNFPA Strategic Plan and the UNFPA GBV Operational Plan, Flourish (UNFPA, 2021b; UNFPA, 2023).

The 2022–2025 UNFPA Strategic Plan acknowledges the impact of digitalization on societies globally, defining it as a global megatrend that cannot be ignored. UNFPA recognizes the benefits of using technology to accelerate progress towards the three transformative results and leave no one behind, while highlighting the necessity of ensuring that technology and digital spaces are safe and equitable (UNFPA, 2021b).

Building on the Strategic Plan, and within the context of digital revolution, the UNFPA GBV Operational Plan, Flourish, outlines TF GBV as a priority to be addressed across the four areas of intervention: response, prevention, enabling environments, and data and research (UNFPA, 2023).

UNFPA based priority planning and programming upon the report Making All Spaces Safe: Technology-Facilitated Gender-Based Violence, published in December 2021. This technical paper contributed significantly to progressing normative frameworks, definitions and programming recommendations on the basis of a comprehensive review of existing literature. Building upon its technical lead in Gender-based Violence Information Management Systems (GBVIMS), UNFPA has further explored what occurs and what can be done at the intersection of GBV programming and technology with its Guidance on the Safe and Ethical Use of Technology to Address Gender-based Violence and Harmful Practices: Implementation Summary. Parallel efforts to increase advocacy and outreach of TF GBV globally have also been established through the successful UNFPA Bodyright Campaign.

The Wilson Center's Science and Technology Innovation Program (STIP) has expertise in emerging technologies and related threats and opportunism, sharing its understanding "through vital conversations, making science policy accessible to everyone". Many of those vital conversations highlight equity and inclusion concerns in emerging technologies and online platforms, such as past work in bringing women in tech to the forefront and how historically black colleges and universities within the United States are engaging in esports and education. Specific to this context, STIP has also supported scholarship central to understanding violence against women online, through Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online. The Wilson Center has also dedicated sscholarship to the broader context of GBV, shown through their work, Accessing Justice: Gender-Based Violence and the Rule of Law.

The Global Symposium on Technology-facilitated Gender-based Violence

The first Global Symposium on Technology-facilitated Gender-based Violence was held during the 16 Days of Activism of 2022, convened by UNFPA and the Wilson Center. The symposium took place online over three days, from 29 November to 1 December, allowing stakeholders worldwide to join the discussions.

This symposium was convened to provide a platform for collective progress in addressing the increasingly pervasive nature of TF GBV and as an opportunity to bring together different fields of expertise from all parts of the globe. Speakers and participants included professionals in academia, cybersecurity, data scientists, activists, civil society, government and non-government partners, United Nations agencies, business and technology, as well as gender and GBV specialists.

Over 90 representatives from more than 25 countries across all regions were actively engaged, as speakers and members of breakout groups, to ensure a truly global discussion. The diverse range of experts in their respective fields brought together the range of perspectives required to meet a common and global understanding of TF GBV and the ways in which it can be most effectively addressed.

Practising "Do No Harm": Within our work we recognize that anyone can become the target of TF GBV; therefore, ensuring the safety, security and privacy of participants, presenters, organizers and observers was taken very seriously. Minimizing risk of exposure to TF GBV meant that this event was invitation only with a diligent check-in process and "day of" contingency plans in place. No recordings were allowed, the online chat was closely monitored and participant information was carefully managed with limited access. There was intentionally no social media before the event to reduce the likelihood of the event being targeted.
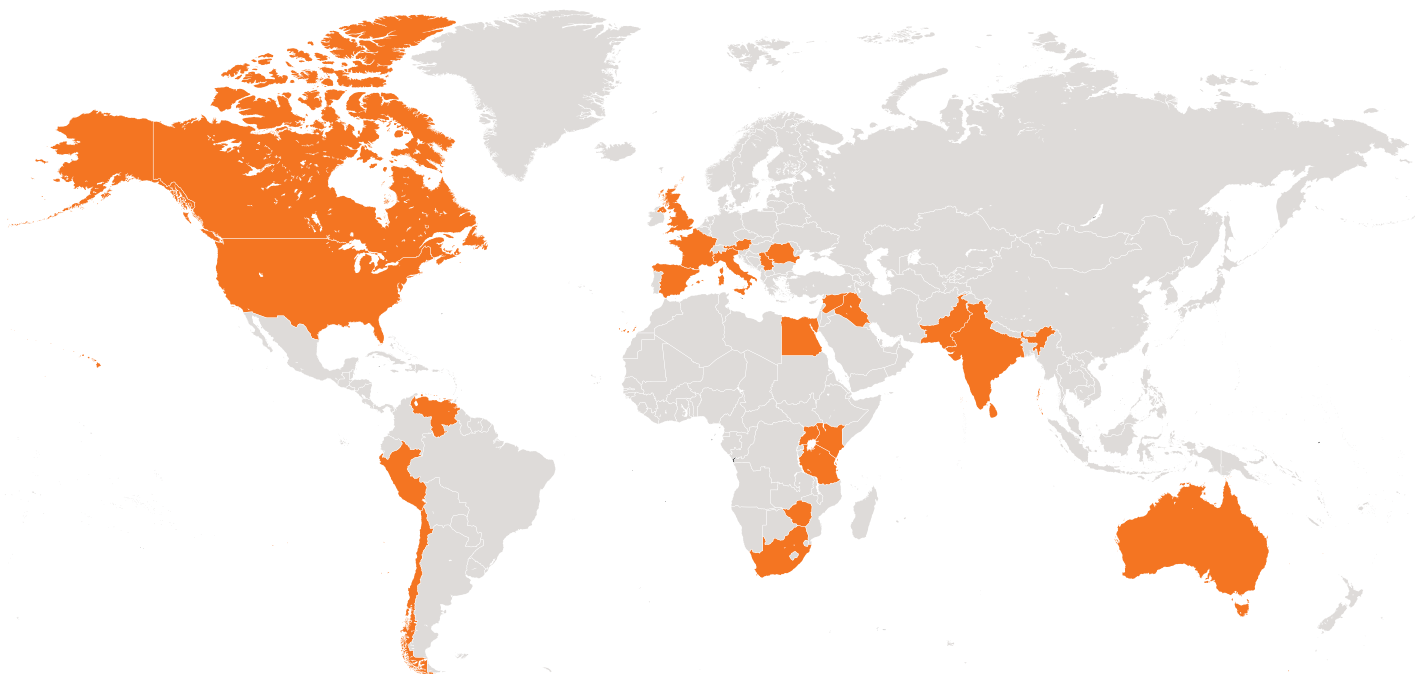
Australia, Austria, Canada, Chile, Egypt, France, India, Iraq, Kenya, Italy, Pakistan, Peru, Romania, Sri Lanka, South Africa, Spain, Syrian Arab Republic, Uganda, United Kingdom of Great Britain and Northern Ireland, United Republic of Tanzania, United States, Venezuela, Zimbabwe

In the months before the symposium, UNFPA conducted a range of consultations with key stakeholders and partners to determine three primary areas of concern that would form the foundation for discussion on each of the three days of the symposium.

1. **Data and measurement, methodology matters:** The first day focused on ethical data principles, practices currently being used across intersecting fields and how they could be applied to TF GBV. Topics explored included data quality, intersectionality, survivor-centred approaches, ethics, safety and security. Breakout sessions addressed information needs, data-collection methods and practices, data storage and management, data analysis, data ownership and dissemination.

2. **Business and technology, feminist Internet:** The second day focused on feminist design frameworks and practices across various areas of expertise and discussed how they can be applied to prevent and respond to TF GBV. Topics centred on exploring Safety/Privacy/Security by Design, AI bias, trauma-informed computing and the default male-centred design of technology. Breakout sessions covered entry points for Safety by Design, adopting a feminist design framework in industry standards, default survivor-centred approaches, community of practice and Global North–South equity.

3. **Law and policy, rights-based regulation:** The last day focused on laws, policies, challenges and rights-based approaches to TF GBV in different contexts. Discussions included issues of self-regulation, national regulation, encryption, survivor-centred policy and future-proofing. Breakout sessions discussed models and processes, backdoor encryption, unintended consequences, overcoming challenges and accountability.

The selected themes built upon a shared agenda, including the Global Partnership and related convenings in protecting, promoting and respecting the rights of women in all their diversity to live free from violence in all spaces.

To ensure that discussions were productive and informed within the rapidly growing field of TF GBV, thought leaders in each of the three different thematic areas were each commissioned to develop a background summary paper highlighting the latest contributions and developments to the field:

Hinson, L. (2022) Technology-facilitated gender-based violence. Data and measurement: Methodology matters. New York: UNFPA.

Hussain, H. (2022) Technology-facilitated gender-based violence. Business and technology: Feminist design. New York: UNFPA.

Venturini, J. (2022) Technology-facilitated gender-based violence. Law and policy: Rights-based regulation. New York: UNFPA.

1. Data and measurement: methodology matters
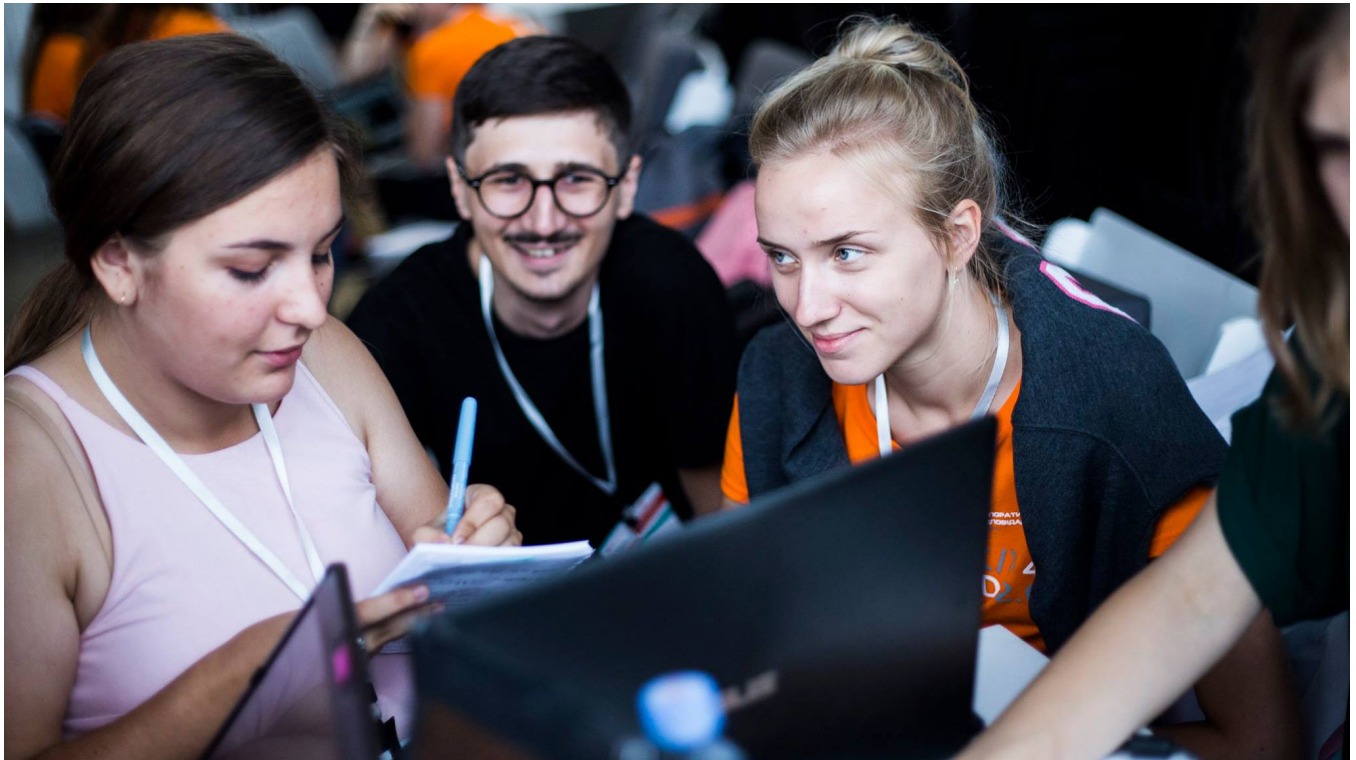
UNFPA Ukraine

Data and research demonstrating the detrimental impacts and extent of TF GBV on survivors and societies are increasingly available. However, standardized and validated tools for safe and ethical data collection that account for the changing and contextualized nature of TF GBV are limited. There is a need for consensus on the intersectionality of the issue, as well as ethics and do no harm approaches in the collection, use, storage and dissemination of data relating to TF GBV.

> **"Data are not neutral, and context and reflection are essential for conducting accurate, ethical analyses and dissemination."**
> Laura Hinson, Senior Social and Behavioural Scientist, ICRW (2022)

The purpose of the session was to build consensus on principles and best practices to ethically decide on TF GBV data needs, and safe and ethical generation, storage and use of that data. This session provided the space to agree upon the foundation for safe and ethical TF GBV data practices, using ethical GBV data guidelines, overall data ethics and data feminism as guiding principles.

Speakers in this session highlighted the centrality of ethics, particularly when it comes to collecting and using data from GBV survivors, including of TF GBV. We heard from experts Kristy Crabtree, International Rescue Committee; Rachel Maxmillian Magege, Pollicy; Lana Ramjit, Clinic to End Tech Abuse; Tarunima Prabhakar, Tattle; and Cheshta Arora, Centre for Internet and Society. Five deep discussions with experts followed presentations and plenary discussion.

Kristy Crabtree, Senior Advisor at the Digital Innovation and Violence Prevention and Response Unit of the International Rescue Committee and member of the GBVIMS global steering committee, highlighted the high sensitivity of GBV data shared by survivors and how this can lead to secondary perpetration of TF GBV. The misuse and unethical management of GBV data, she explained, is

likely to cause further harm to survivors, and the consequences are severe: social isolation, stigma, reduced psychosocial well-being, physical retribution and even death.

> **"Ethics of data are complicated and ever evolving, especially in [the GBV] field, where we have to acknowledge the likelihood and severity of risks if that data is misused."**
> Kristy Crabtree, International Rescue Committee

Tools and practices in the GBV data and technology space are changing. Ethical and safe sharing of data is certainly beneficial to inform programmes, mobilize resources, and improve advocacy and service coordination. However, there is a persistent gap in understanding the privacy and security risks involved with collection, use and dissemination of GBV data. Indeed, "[s]ometimes even bad practices are promoted". She also spoke to the central question of whether and for what purposes the data need to be collected in the first instance. **Collection of data around GBV attracts risk of harm** and a balance in determining need against risk must be made.

Crabtree suggested three key principles to minimize risks when talking about GBV data:

- Do no harm. Situations of data sharing create additional harm for individuals in a very real way.

- Consider the effects on help-seeking behaviours. Negative experiences with data sharing can reduce overall help-seeking behaviours by survivors.

- Consider the safety of staff and organizational reputation. When confidentiality is violated, staff may be threatened with physical violence and stigma, as well as the reputation of the organization.

Rachel Maxmillian Magege, Lawyer and Projects Associate, Pollicy, drew the links between digital extraction in Africa and an enabling digital environment for TF GBV, adding a new and key dimension to the

data ethics discussion. She condemned extractivist practices by technology companies, who establish their platforms in the African continent and use them to collect wealth in the form of data and information, which is then unethically shared and used for profit and personal gain without any return for users and communities. Magege detailed the nine ways in which digital extractivism manifests[2] and how some of these can foster TF GBV. It is crucial that our TF GBV data-collection methods do not replicate or exacerbate extractive data practices simply because it is the status quo within the current profit-driven technology industry.

> **Panel Discussion:** How do we empower survivors instead of abusers, in relation to freedom of speech and expression?
>
> As Lana Ramjit pointed out: we "need to have the concept of ownership of [our] profile online." Perpetrators may be able to distribute harmful content online, but taking ownership of that content is very difficult. Survivors have no right to remove abusive content or data. Hence, platforms tend to favour abusers, while blame is usually put on the survivor for not taking action to prevent abuse. "We have to put the responsibility on the abusers and change the normative construction of blame."
>
> Tattle, through the tool Uli, is "actually doing something that the platforms should be doing." Prabhakar highlights their advocacy work, and how they are "speaking up to the platforms [to demand] to do more in creating solutions for violence online".

Data ethics considerations underpin the work of the Clinic to End Tech Abuse (CETA) and Tattle, two organizations that use different approaches to collect TF GBV data while placing survivors at the centre of their work.

CETA is a tech abuse clinic that works as a research communication and policy hub, focused on the intersection of intimate partner violence (IPV) and

---

2   (1) Digital labor, (2) illicit financial flows, (3) data extraction, (4) natural resource mining, (5) structured monopolies, (6) digital loaning apps and technologies, (7) funding structures, (8) data testing and (9) platform governance.

technology. Lana Ramjit, a Computing Innovations Postdoctoral Fellow at Cornell Tech and CETA's Director of Operations, described how the clinic started as a research study on the use of spyware in situations of IPV, which raised ethical concerns on conducting data collection without established response mechanisms to support survivors. This led CETA to address their own collection of TF GBV data and provide trauma-informed services to survivors. Currently, CETA's research and advocacy work strictly follows GBV data principles and data ethics and prioritizes survivor-centred provision of prevention and response services. This means service provision is prioritized over research and incident data are only collected with survivors' consent. Ramjit detailed how CETA continually updates their protocols and referral systems in consultation with IPV experts, ensuring that the advice they provide is targeted to individual survivor's situations, and how they have successfully advocated for survivors' needs and appropriate policies and laws. In order to support other organizations to set up their own tech abuse clinics at the local community level, Ramjit announced that CETA will be releasing a toolkit and guide; this has since been published.

> **Panel Discussion:** How can we move from incident reporting of TF GBV to build a data-collection ecosystem that involves different systems, tools and communities?
>
> Magege warned about the need to be very careful when collecting data and digital information. While Pollicy conducts research on TF GBV, this is not an easy task given platforms' biases. She claims that the existence of regional frameworks could provide digital sovereignty and recommends collect[ing] data from different stakeholders on a regular basis.

Uli is a survivor-centred tool designed to mitigate TF GBV on Twitter and was developed by Tattle, a community of technologists, researchers and artists working towards a healthier online information ecosystem in India. Tarunima Prabhakar, project manager and co-founder at Tattle, and Cheshta Arora, researcher at Centre for Internet and Society that supported Uli, described Uli's functioning and how it is being used to build a survivor-owned evidence base.

Uli was developed as a response to the limited investment put into content moderation in languages other than English, including Indian languages. According to Prabhakar, this disproportionately affects marginalized voices, particularly Indian women and politicians, who are subjected to online harassment.

> **"The everyday nature of TF GBV is often ignored, and people suffer in silence. Can we respond to this everydayness through a user end intervention? Uli wants to empower people to coordinate response to online GBV and emphasize the feasibility of safety tech in Indian languages."**
> Tarunima Prabhakar, Tattle

Uli is a browser-based plug-in for Twitter, co-designed with over 30 activists and researchers. Through a crowdsourced list of slurs in Indian languages and machine learning, Uli filters and detects harassing, hateful language and online GBV and hides problematic posts from a user's feed. It also allows users and activists to archive content which is a useful function to save data relating to the incidence of usage as evidentiary material for tech company and justice system responses. The browser extension also calls on networks for action and offers mental health-related information.

Panel Discussion: What about contextual language and content moderation?

Prabhakar and Ramjit agreed that human content moderators are essential to recognize abusive language, which can be highly contextual within communities and relationships, and take corresponding action.

> "Sometimes machine learning [content moderation algorithms] flattens the context. The solution could be to keep the human voice alive through all the automated systems. Tattle is planning to obtain descriptions from people on why they think certain words or photos are considered abusive, in order to understand why some words are considered slurs."
> Tarunima Prabhakar, Tattle

> "Some words that are seen or considered as abusive from the outside of the partnership can be considered as a threat to violence within the relationship. When trying to report these words they can lose their context. Therefore it is important to keep humans in the loop for adding back to the context."
> Lana Ramjit, CETA

> "Pollicy conducted research on discriminatory language online and dominant language in certain digital spaces. We found that brown and black people would be reported more often, and more actions would be taken against them."
> Rachel Magege, Pollicy

Following the presentations, participants and experts in the field further discussed ethical and other considerations in every step of the data-collection process: determining information needs, data-collection methods and practices, data storage and management, data analysis, and data ownership and dissemination. The following are key points from each discussion.

Information needs

- **We need more consistent, reliable data.** Most available research and evidence has been collected in high- and middle-income countries, with a strong focus on non-consensual sharing of intimate images and technology-facilitated violence against women journalists and human rights defenders. Participants highlighted the lack of consistent and comparable data and research on other, less visible forms of TF GBV, and the need for further research using intersectional approaches and focusing on other geographies and contexts, including humanitarian settings.

- **Ethical and survivor-centred data needs.** The point was made repeatedly that the risk of harm to survivors cannot outweigh the purpose and need for data and research. The purpose of the data collection needs to be well understood by those it is being collected from. Very often, data needs fall into a need for evidence-based advocacy as opposed to evidence-based laws, policies and programmes. If data are to be collected, it must be with survivor-centred and do no harm approaches, including ensuring the availability of services specifically capacitated to support survivors of TF GBV.

- **Data for action.** There was clear consensus that collecting data for research purposes alone does not justify the risk of harm. Data need to be targeted towards advocacy, policy development and programme implementation. Current knowledge can support effective design and implementation of policy and legislation as well as programming interventions to stay abreast of emerging technology and trends. Similarly, evidence on what works to address TF GBV could inform the establishment of regulatory bodies or commissions to bridge survivor experiences and accountability of social media platforms and technology companies.

- **Data for influence.** New research and data on TF GBV need to be generated and used to influence prevention, safety and safeguarding actions by technology companies and social media platforms, service providers, NGOs/civil society organizations (CSOs), governments and other regulatory bodies.

Data-collection methods and practices

- **Diverse data-collection methods.** Prevalence data on GBV and TF GBV are primarily being collected through population-based surveys. The GBVIMS is being adapted to support collection of incidence data relating to TF GBV. Smaller-scale surveys, interviews and focus group discussions are also used to capture subgroup realities of online experiences. However, there is not enough data collection across all groups of product users, including women and girls at the intersection of various forms of discrimination, due to the difficult nature of researching TF GBV.

- **Increasing popularity of remote and digital data-collection practices.** Participants highlighted the increasing use of remote data-collection methods, namely phone-based and web-based surveys, which have raised some ethical concerns. These practices could potentially be harmful, due to the difficulty enumerators have in recognizing distress (phone-based surveys) and the inability to ensure privacy. The lack of contextual information at the time of remote data collection may increase the risk of severe violence. Further, it is important not to shift fully to digital collection practices, since remote data-collection methods risk leaving marginalized populations behind, particularly those without digital literacy and access to technology devices such as phones or the Internet.

  > "The distress of women, their body language, cannot be read through remote data-collection methods. How is the well-being of women put at risk or even worsened when using these methods?"
  >
  > Participant and a researcher at a multilateral United Nations organization

- **Ensuring participant safety.** Tension between the inclusion of vulnerable populations and the safety risk to participants in research is an important and central consideration. Internally displaced people, members of the lesbian, gay, bisexual, transgender, queer or questioning, intersex, asexual, and more (LGBTQIA+) community, individuals with lower digital literacy and other women in all their diversity face disproportionate risks when engaging in research. While researchers may understand the value of this data for advocacy and programming purposes, careful attention must be paid to ensuring participant safety and avoiding misuse of collected data. Suggestions included working through local NGOs and community-based groups, who have the capacity to provide responses to TF GBV and have an in-depth understanding of the issues and the impact.

- **The importance of consent and the right to be forgotten.** There is a need to move away from an external ethical review board type of consent to one that encapsulates authentic consent. According to participants' experiences, some consent techniques are particularly helpful when collecting data related to GBV, including breaking consent down into its components, ensuring colloquial descriptions of technical language, allowing time for participants to consider the information and decide, and considering consent as an ongoing process by reminding participants that they can withdraw at any time. Participants also discussed the need to include issues of data storage during the consent process and the right for participants to have their data deleted at any time.

  The use of big data, AI and machine learning as sources of data collection is concerning, as this process erodes the role of informed consent and may introduce biases.

Data storage and management

- **The risks of poor data storage and management.** There are several risks associated with certain data management and storage practices, including sharing of data between advocates, service providers and donors.

  > "As advocates, we are so worried about getting [immediate] needs met that we may ignore the more abstract concerns. For example, a physical threat of violence versus someone's full address on file."
  >
  > Participant from a United States gender-based violence and technology civil society organization

  > "Communication over a specific case might happen between organizations and persons through messages, voice messages, revealing personal information when consent has not been received to share their story. This is one way through which data travel, but also the way we do networking and solidarity work."
  >
  > Participant and manager of an international digital rights civil society organization

  Sharing of survivors' data and information may lead to the creation of an ad hoc data set, which may include information traces that can identify survivors and cause further harm. There is a critical need to understand and identify the nature of the data and how a breach of data can be harmful for survivors and organizations.

  > "I heard about this practice, [in a small Asian country], where people take in cases and type out everything the survivor shares and then share all the details from the survivor for legal proceedings. This helps survivors since they don't need to relive the story again, but how do we deal with the traces left from this?"
  >
  > Participant and manager of an international digital rights civil society organization

- **Protocols and practices for safe data storage and management.** While researchers, service providers and advocates may have different needs in terms of data management and storage, participants agreed upon the need for policies that regulate data management and storage. A number of safety principles must be embedded:

  1. **Encryption and anonymization.** Files that are shared and stored need to be encrypted, secure file transfer protocols for data exchange need to be established and identifiable information, such as names or organizational aspects, should be removed.

  2. **Data storage.** Data may be stored in safe servers, but never online, to avoid data breaches. Data sets need to be split and stored in separate files in different and disconnected databases.

  3. **Control of data.** There must be control around who has access to the data and encryption. It is important to ensure that those who have access to the data have a genuine use for the data and are compliant around usage.

  4. **Timelines for data destruction.** Data should not be kept for longer than necessary and records should be destroyed as soon as possible. In research, in particular, the data storage plan needs to detail the timeline for data destruction, although there is no auditing to verify that destruction. Ethical review boards should require a data destruction timeline and verification that data were destroyed.

- **Training advocates and service providers.** In the United States, Front-line service providers are often not trained to deal with issues of data safety and sensitive information. A United States gender-based violence and technology CSO, is training providers on safe data management practices as outlined above.[3]

Data analysis

- **Countering data bias through self-reflection in analysis and reporting.** As with all research, there is a need for self-reflection and acknowledgement of the researcher's own bias and how these may impact upon the research process and analysis. Strategies for data triangulation and transparency are required, including the involvement of various stakeholders to choose appropriate frameworks and questions without being heavily influenced by a priori assumptions; or the need for transparency and constant reflection on decisions made, research limitations and internal biases.

  > "Many people have talked about their experiences in technological abuse (harassment, stalking), but people don't always identify this as abuse. Especially online, our narrative of other people's experiences might differ from how people identify their own narratives."
  > Lana Ramjit, CETA

- **Survivor-centred analysis and safeguarding mechanisms.** "Every data point is a real person's lived experience."[4] Holistic and survivor-centred approaches to data analysis are key to ensuring the lived experiences of survivors are accurately reflected in results.

> "I'm thinking about the role of the specific types of trauma that come with technology-facilitated abuse. We don't want to use people's narratives in a way that is hurtful to them, or that they don't agree with, but that's also really hard when we're talking about things like hypervigilance and paranoia."
> Lana Ramjit, CETA

Survivor-centred approaches also mean establishing safeguarding mechanisms to protect informants from retraumatization and further harm due to deanonymization.

There is a need to create a space in the research process to provide support to survivors and make these processes less extractive.

- **Gaps in analysis of experiences of marginalized populations.** Significant concerns remain related to the likelihood of missing experiences of those most at risk of TF GBV. Barriers such as language, lack of cultural and contextual knowledge and limited access of marginalized communities to essential GBV services hinder understanding of TF GBV among certain communities, such as Indigenous and First Nations people.[5] Similarly, people with diverse gender identity, undocumented people, people living with HIV and people who use drugs are particularly vulnerable to being left behind in TF GBV research. It is critical to ensure data and research findings and conclusions are validated by those who contributed to the research, including participants and communities.

---

3 Participant from a United States gender-based violence and technology CSO

4 Participant working for a United States research, design, and art agency

5 Participant working for an independent regulator for online safety

Data ownership and dissemination

- **Survivors' ownership and control over their own data.** Data are currently considered to be owned by companies, organizations and governments, but as our entire lives are increasingly lived online and our bodies become more digital, we must stop and question who should have the rights to data. Data ownership is nuanced and, while open data and collective ownership, for example, are certainly useful for advancing scientific research, they may also come with risks such as increased abuse, issues of confidentiality and exploitative use of survivors' data. Companies of all sizes are collecting TF GBV data without survivors' knowledge or consent. There is a critical and urgent need to address the lack of knowledge around data rights by general users and survivors of TF GBV to establish responsible data practices. There is also a need for increased engagement with the private sector, technology companies and women to co-develop feminist data principles. These would ensure safe and ethical sharing of TF GBV data, as well as prioritizing survivor-centred engagement and inclusion, prioritizing their agency and participation.

- **Limited and unequal funding for good data practices.** Opaque and unethical data practices endorsed by technology and private companies exist, while funding for good data practices in NGOs is limited and unequal. Funding and resource inequalities undermine the ability of NGOs to set up strong data security and protection measures. There is a need to address funding structures to aid the development of a feminist Internet and allow the proliferation of tech that supports survivor data to influence strong tech companies.

- **Dissemination for movement building.** Social movements are critical in the design of advocacy strategies that ensure intersectionality, confidentiality and information-sharing on TF GBV. Data experts and researchers need to work with users to create cross-functional and interdisciplinary teams to address issues of gendered misinformation, data exploitative practices and harmful use of data, all of which can lead to TF GBV.

Key takeaways

1. TF GBV data practices must be grounded by global GBV data ethics as a minimum. They should then be further expanded upon given that digital collection, use and management of digital data bring even higher risk than purely analogue.

2. Care should be taken that TF GBV data practices do not replicate extractive data-collection practices, common within the technology industry.

3. Risk of harm to survivors should always be given more importance than any potential benefit for data and research. TF GBV data collection should not take place unless participants' safety can be ensured, specifically there must be TF GBV response services established.

4. The understanding of data ownership must shift from something that a company, organization or government can indefinitely own to something that is an extension of the human, requiring fully informed and ongoing consent for their storage and use.

5. Consent must be an authentic and ongoing interaction, not a one-off exercise.

6. Unethical generation, management and misuse of data may lead to TF GBV, including data collection on TF GBV specifically.

7. More evidence is needed on TF GBV, especially in low- and middle-income contexts and in humanitarian settings.

8. Do no harm, survivor-centred, intersectional and participatory research processes must be adopted across all steps of the research/data process: from defining needs to data collection, analysis and dissemination.

2. Business and technology: feminist Internet

There is growing recognition that the surge of TF GBV is rooted in the gendered power imbalances and business models that govern technology companies. Women and feminist perspectives have been systematically excluded from product development, leading to unsafe products, policies and services for women and marginalized groups, placing survivors of GBV at risk.

> **"As everyday technology use becomes the norm, the harm posed and perpetuated by technology designed for the 'default male' user deepens."**
> Hera Hussain, CEO, Chayn (2022)

This session provided the opportunity to build consensus on best practices for ethically engaging and dismantling harmful business practices and systems incorporated in technology design that perpetuate TF GBV. It laid the groundwork for the application of feminist design frameworks and approaches to technology and cybersecurity to prevent and respond to TF GBV.

Means and methods were outlined for the ways technology is harmful and unsafe for women, girls and marginalized groups. Examples of feminist and survivor-centred technology tools that address TF GBV were also showcased. We heard from experts Kat Lo, Meedan; Hera Hussain, Chayn; Tracy DeTomasi, Callisto; two product safety experts, Apple; and Mayana Pereira, Microsoft. Following the presentations and plenary discussion, there were five in-depth discussions with experts.

Kat Lo, Content Moderation Program Lead at Meedan, described the ways in which experiences of online violence and harassment are often not addressed but can be integrated into technology products and platform policies. "Any target of abuse must conform to how the system understands abuse in order to be seen or heard," she stated. Indeed, certain forms of online violence, such as stalking

or harassment campaigns, do not exactly align with platforms' policies on what constitutes abuse, thereby leaving survivors unheard and unprotected as algorithms fail to detect abuse and content moderators lack information to respond.

To avoid retraumatization of survivors and ensure an effective response to cases of abuse, Kat has developed a set of guidelines for CSOs, academia and policymakers to understand and enforce content moderation accountability on social media platforms.

Further, survivor-focused industry standards to prevent abuse are urgently required while bearing in mind certain considerations and trade-offs for their development and implementation (Table 1).

Table 1. Potential considerations when making survivor-focused industry standards and products. Adapted from presentation by Kat Lo: "Yelling into the void: from managing online abuse to designing safer platforms."

Transparency		Privacy
Transparency		Gameability
Better monitoring to detect abuse	versus	Building infrastructures of surveillance
Faster moderation response time		Greater nuance and context
Address local context for hate, abuse, law		Consistent, auditable global standards

Four industry standards were proposed: (a) provide a reporting option for every social interaction feature on the platform; (b) require a protocol to audit new features for abuse potential and an analysis of reporting mechanisms; (c) create the possibility to pre-emptively block users, including from their profile page, and (d) introduce paid programmes to integrate advocacy organizations into product development.

> **"Companies need to hire people to focus on TF GBV and safety online as a whole to ensure seamless integration and consistency in progress made."**
> Kat Lo, Meedan

Principles of survivor-centredness and trauma-informed design underpin the work of Chayn and Callisto, two startups that address GBV and tech abuse using technology innovation.

Hera Hussain, founder and CEO of Chayn, described the power of open-source technology, trauma-informed design (Hussain 2021) and hope-filled framing to create web-based resources to address GBV and technology abuse. Based on the work of Chayn and the recent development of the guidelines Orbits, eight principles were highlighted to advance the intersectional, survivor-centred and trauma-informed design of technology and interventions to address TF GBV:

1. **Safety.** Making brave and bold choices that prioritize the physical and emotional safety of people.

2. **Agency.** Honouring the survivor's wishes to create affirming experiences. This requires seeking informed consent at every step and providing information, community and material support to survivors.

3. **Equity.** Designing for inclusion. This must consider how position, identity, vulnerabilities, experiences, knowledge and skills shape trauma and recovery. Survivors are not a homogeneous group.

4. **Privacy.** Respecting and understanding privacy. Due to the stigma, victim-blaming and shame associated with GBV, there is a greater need for privacy. A survivor's personal information, including their trauma story – such as data, images, videos or statements – must be kept secure and undisclosed, unless the survivor decides otherwise. At the same time, we should remove unnecessary obstacles to users getting to the information and help they require. In an economy where the currency of interactions is data, we must consider the harm we may introduce from intrusive data collection, storing and selling in technology design. This involves understanding that some vulnerable groups will be unable to foresee the risks arising from their data.

5. **Accountability.** Maintaining a relationship of trust; being open and consistent about what is being done, how and why. We must create and nourish constructive feedback loops that trigger changes in law and policy related to tech abuse; place a duty of care and minimum standards on industry and tech companies to ensure that they have adequate infrastructure to prevent tech abuse and support survivors; create laws that recognize the cross-border dimension of tech abuse and have provisions on how to navigate this borderless crime; and develop institutions to facilitate access to non-criminal remedies.

6. **Plurality.** Actively leaving space for complexity and recognizing that harm manifests in different and disproportionate ways for people living at the intersection of multiple oppressions.

7. **Power redistribution.** Distributing and sharing power by safely co-designing interventions with survivors.

8. **Hope.** Creating validating, empathetic, warm and soothing experiences, motivating people to seek and embrace the help on offer. We should seek collaborative solutions and offer hope for the future.

Implementing these design principles will assist developers in testing, rationalizing and questioning their products. It will serve as a guide for developing effective and useful trauma-informed products.

Callisto Vault, a survivor-centred and feminist design app, is an example of how technology can be ethically used to respond to the needs of GBV survivors (Callisto, 2023). As Tracy DeTomasi, CEO of Callisto, described, Callisto is a "suite of tools designed to help survivors navigate barriers and define their own pathway towards healing and justice". Used on college campuses, where over 90 per cent of sexual assaults are committed by repeat predators, Callisto addresses the common feeling of loneliness experienced by survivors. In Callisto, DeTomasi's team has designed a matching system through which survivors can enter the perpetrators' social media information to find out whether someone else has been attacked by the same repeat offender. Then, "each survivor is connected with a Legal Options Counsellor, a third-party attorney who will explain their options and facilitate coordinated action, while protecting survivor privacy". Callisto Vault's second tool is an encrypted record form that allows survivors to document their experience, while deciding their next steps. Each of these tools are crafted to prioritize the needs and privacy of the survivor while they decide which course of action, if any, is best for them.

Panel discussion: Safety versus security: does having user data help or hurt survivors?

"We need to take a human rights lens to prevent the surveillance apparatus that is built to monitor and protect [being] used against the same vulnerable people it was designed to safeguard. Survivors are more than the trauma they have experienced."
Hera Hussain, Chayn

"Many survivors want to give more context to the moderators about why they are reporting, which in turn leads to providing more information. There are concerns about governments asking for information from social media, so people are very reluctant to report, because the data can be tracked, for example data on LGBTQIA+ people in places where they are persecuted."
Kat Lo, Meedan

"We need to work with informed consent, and let people know exactly how we are using the data in every step of the process, so that they can make the choice."
Tracy DeTomasi, Callisto

Not only are small startup companies addressing TF GBV, large technology companies, such as Apple and Microsoft, have also developed mitigation strategies and tools to prevent TF GBV from occurring in their platforms and through their products.

"Many people share their passwords with their partners, but in abusive relationships it's difficult to determine whether this was done in good faith. Technology is an essential tool in people's lives, including survivors, as they use it to find information on support and access to safety."
Senior Product Safety Advisor, Apple

Acknowledging that a one-size-fits-all approach to TF GBV does not work, Apple focused on speaking to a myriad of transparent safety solutions for survivors that were developed in consultation with networks of TF GBV front-line service providers.

Apple's tool Safety Check (Apple Support, 2022) allows iPhone users to see who has access to their information and how much information other users can access, what information users are sharing with various apps, and which devices are connected to their profile, as explained by a product safety engineer and senior product safety advisor at Apple. Safety Check helps users navigate how to change their settings quickly if they are experiencing TF GBV, and how to manage sharing access and protect their passwords and information from someone they no longer want to share it. In the design process, Apple carefully considered three aspects: (a) ease of use, to ensure flows are agile and meet survivors needs quickly; (b) transparency, to provide insights into how users are connected to others; and (c) control, to prioritize survivors' information-sharing options.

Mayana Pereira, Data Scientist at Microsoft AI for Good Research Lab, shared other ways large technology companies can leverage their expertise and support the work to end TF GBV. She provided an overview of two safeguarding technical tools that Microsoft have developed and how these can be used to prevent and detect TF GBV. First, SmartNoise library is a tool used to anonymize and privatize data. That is, when public data are shared, such as a restaurant review, SmartNoise de-links information from individual users, allowing the dissemination of anonymized data sets, preventing the disclosure of sensitive information and reducing risk exposure. Another tool, differentially private synthetic datasets, uses AI to generate a new set of anonymized data that preserves the distribution of the original data received from users. These synthetic data sets can then be used for machine learning purposes to, for example, detect instances of child sexual abuse or GBV. Both these tools have the potential to be used safely and ethically as an ally in digital safety and to understand the prevalence and nature of TF GBV. In turn, this can make survivors more comfortable sharing information while protecting their identity.

Panel Discussion: What are the biggest gaps in technology/products with respect to tech-facilitated GBV? Where should the focus of efforts be now and in the near future?

"New platforms are not prepared for moderation. Companies endeavour to have exponential growth and then establish safety mechanisms afterwards. But, in reality, it is not a staggered process. Companies need to embed safety protocols in design from the start, and it is important to generate good practices to create industry standards."
Kat Lo, Meedan

"Independent services can help build moderation and strategies for multiple platforms. We should not accept secrecy, where platforms do not allow for exchange or for services to work with multiple apps."
Hera Hussain, Chayn

How do we bring all parties together to solve this, NGOs, research, platforms, policy?

"Funders have an important role to play in defining standards, we must make time for the conversations."
Tracy DeTomasi, Callisto

"Many platforms focus on national organizations, especially in big organizations in places like the United States. UNFPA and other such organizations can serve as equalizers, to target power differentials of who are getting included and who are not."
Hera Hussain, Chayn

Once expert presentations concluded, there were deep discussions by a cohort of experts. Key elements for consideration around five themes at the intersection of technology and feminist principles were identified. These themes included: entry points for Safety by Design, feminist design frameworks for industry standards, survivor-centred technology by default, community of practice and Global North–South equity.

Entry points for Safety by Design

- **Policy and economic deterrents.** Currently, companies have no incentives to implement Safety by Design, particularly if these mechanisms contribute to profit cuts. The business model of technology companies prioritizes profit, often at the expense of safety, as evidenced by the experiences of some participants.

> "In the for-profit world, people were worried about how policy would impact their profit margins, so it was difficult to make the argument unless there was a profit threat."
>
> Participant from a United States gender-based violence and technology CSO

It was agreed that, in general, trust and safety is expensive to enforce for companies, and many have turned these procedures into a "box-ticking" exercise with limited to no impact on their users.

> "We have a collaboration with a social media company to look at their internal trust and safety procedures and how these affect offline violence, but our recommendations went nowhere. It was simply a 'box-ticking' activity."
>
> Participant from an international GBV organization

External regulation and public policy are a key entry point for large-scale change. Governments should design and enforce implementation of tools and mechanisms that prevent harm through the development of policies and regulations, while providing an enabling environment for sharing of knowledge and expertise across companies, industries and borders.

- **Internalization into core values.** Safety by Design needs to be integrated into companies' internal values, while considering the specificities of each company and each product. That is, to ensure sustainability of Safety by Design approaches, these need to be integrated within the company's business model.

- **Normalization through education.** Subjects of ethics and consent need to be incorporated into computer science and software engineering courses, to ensure understanding of ethical questions among those who build technology.

- **Transparently engaging with users.** Technology companies should engage end users, particularly women and girls, CSOs and marginalized communities from ideation and design stages, and continuously through feedback loops on their products. In this regard, they must invest in human resources to nurture relationships with these groups. Further, there is a need for transparent, accessible and understandable language in all safety features of the product, including when seeking users' informed consent.

- **Design for the margins.** When technology products are created to meet the needs of a group of selected "model" or stereotypical users, they will systematically exclude and fail to address the needs of many others, particularly those who are marginalized and are exposed to increased safety risks. Thus, safety precautions must be tailored not only to the specific industry or product, but also to tackle the hardest safety problems. As a participant and CEO of a United States technology company expressed, "do not build for the bell curve, build for the margins. [...] If you solve the hardest safety problems you can solve the rest".

Feminist design frameworks to industry standards

- **Clarify feminist design.** There is a false assumption that computers cannot make decisions that are sexist, racist and non-inclusive. Computers and data sets do not have opinions or preferences, but the humans who build them do. The more we rely on decision-making algorithms and computers, the more likely a seemingly small bias will exponentially amplify. Having a diversity of perspective is essential to achieve feminist design.

- **Coalition building for safety.** There needs to be more collaboration and coalition building outside of the traditional security lens to come up with solutions that keep all users safe. Security tactics, methods and theories largely come from defence or military perspectives, both of which are heavily masculine. IPV and other forms of GBV require a different perspective to ensure the safety of survivors; therefore having a diversity of voices in the room is central to recognizing and addressing these problems.

- **Context adaptation is key.** Current standard-setting organizations within the technology industry are led by and focused on high-income countries, but harm is felt globally. Those in decision-making positions must, at a minimum, consider different global contexts and languages. Ideally, more global diversity is needed within these organizations and regional standards should be considered. Special attention should also be given to how products are designed, with a particular focus on shifting responsibility away from users.

Default survivor-centred

- **Technology companies at the front-lines.** Participants described how survivors of TF GBV often rely upon content moderators and customer services for assistance. This results in a reliance upon staff in tech companies to provide an informal GBV front-line response without adequate training and support.

   > "I've seen a lot of moderators provide informal therapy for people dealing with intimate partner violence, self-harm and eating disorders, far outside the scope of what they can do safely for themselves and others."
   > Kat Lo, Meedan

   A participant and director of a large cybersecurity company confirmed that some companies have responded to these needs by training their customer support staff on how to manage complex violence situations. Tech companies should consider and plan for their users to be survivors, and in particular, work with GBV experts throughout the product lifecycle.

- **Survivors over profit.** Survivor-centred technologies require work, time and money. They need unconditional funding that is accountable to survivors themselves rather than to the companies and investors. This requires a change in business models, where survivors' data are not used for profit and where technology is built to anticipate and address potential harms by default.

- **Intersectional and trauma-informed approaches to technology.** Survivors of TF GBV are not homogeneous, and have different identities, needs and behaviours, speak different languages and live in various contexts with specific cultural characteristics, all of which affect their experiences of TF GBV. Any technology that is survivor-centred needs to consider the intersectionality of

survivors, and it must be [trauma-informed (CDC, 2020)](#). This requires collaboration with advocates, organizations and experts across multidisciplinary sectors, including technology and GBV sectors.

Community of practice

- **Need for standardized terminology, accurate data and evidence for best practices.** Reiterating similar views as expressed during the first session of the symposium on data and measurement, participants highlighted the lack of in-depth and good-quality data on the prevalence and impacts of TF GBV on marginalized populations. In addition, they highlighted the lack of available evidence on the effectiveness of existing prevention and mitigation strategies across a variety of contexts, including humanitarian contexts. These are central to working towards evidence-based interventions to ensure survivors' access to services, governments' investment in response and prevention services, and facilitation of cross-fertilization and learning from the experiences of others.

  > "We use the community to connect with our partners through the Internet, and this space is open to the public. So, there may be a disconnect between a survivor who searches "my boyfriend shared my photo" and the language we use. We may need a different kind of language to get to the wider community."
  >
  > Participant and manager of international digital rights CSO

Recognize power imbalances in the community of practice. Power structures and power imbalances within the community of practice need to be acknowledged and addressed. This means survivors must be put at the centre of the community of practice work, and existing North–South divides bridged in knowledge translation.

- **Principles and functions of the community of practice.** The discussion outlined eight principles to guide the community of practice: feminism in ethics and approaches, survivor-centred and trauma-informed approaches, user empowerment and agency, responsibility of service providers, transparency, accountability, Safety by Design and equity. Similarly, and in line with these principles, participants debated some of the potential roles of the community of practice, including being an accessible space for survivors, validating TF GBV data, bridging the gap between disconnected stakeholders (policymakers, researchers, GBV practitioners, etc.), improving the digital literacy of marginalized groups, and fostering user-led approaches to technology development by working with technology companies.

Global North–South equity

- **Differences in digital literacy and access to technology.** The differences in digital literacy and access to the Internet between the Global North and the Global South make it difficult to engage in discussions about equity and to address power imbalances collaboratively. These differences further reinforce the problem: limited access to technology in the Global South means limited opportunities for learning and growth, and limited infrastructures and resources mean less data to inform solutions to address digital illiteracy. Additionally, within countries, urban and rural digital divides are being obscured, and a focus on rural areas remains important, as highlighted by a participant from a Peru CSO.

- **Working to address TF GBV in different contexts.** To ensure equity across contexts and empower people to create solutions, despite their location, it is important to democratize funding and facilitate connections between TF GBV activists and organizations. This must take an equity-based approach to avoid reproducing existing power imbalances. For example, providing technical support and resources to small and local organizations that work on TF GBV to pilot their solutions, facilitating direct collaborations of stakeholders across contexts, and respectfully amplifying their work globally were some of the strategies that arose in discussions.

- **Proactively addressing tech monopolies interest in the Global South as new markets.** Vulnerable users with low literacy who may not have the economic ability to purchase data packages are being offered low-cost or no-cost options (e.g. Facebook Basics) in exchange, often unbeknownst to them, for their data. This has created concern, as expressed by a participant:

  > "Working with partners in Africa, many of them have concerns about their data safety. However, with limited access to platforms, and monopolizing of the Internet by specific companies, there is limited room for them to do anything about it."
  >
  > Participant and cybersecurity research fellow from a United States university

These practices are likely to reproduce power imbalances unless concerted action is taken to stop the expropriation and exploitation of marginalized users; solutions offered in the discussion ranged from raising awareness of tech monopolies and establishing practices of authentic informed consent in contexts with limited access to information.

Key takeaways

1. Understanding and incorporating survivors' needs throughout the product lifecycle by integrating women and girls' input into technology products, processes and systems is necessary. Ethical and safety standards for GBV data do not recommend directly interviewing or collecting data from known survivors unless minimum standards are met and in place.[6]

2. There is a need to identify and work to counter all power imbalances.

3. A holistic assessment and shift of the business status quo is necessary for women to be safe, including core functions, business models and operations of technology.

4. Innovative approaches and ideas, grounded in offline GBV normative frameworks and expertise, are necessary to ensure the proper safety of women and girls in the digital age.

5. There is a need for industry standards grounded in global experiences and intersectional perspectives to support the technology industry and more easily regulate for safety.

6. Safety by Design, survivor-centred and intersectional approaches in technology development must be enforced from the beginning, and integrated and normalized throughout tech companies' processes.

7. Multidisciplinary teams are best positioned to address TF GBV holistically. Partnerships and collaborations across sectors are central to properly understanding and creating effective solutions.

8. Context is crucial to understanding, preventing and adequately responding to TF GBV globally.

9. Survivor-centred and trauma-informed technology to respond to TF GBV and offline GBV can be ethically developed, and examples of good practices exist.

---

6   Best practice is to interview and collect data from women, knowing that one in three women has experienced GBV in their lifetime. Treat every woman as a survivor, but do not ask specifically if they have been subjected to GBV. This information is often not necessary and immediately increases risk of harm to everyone involved.

3. Law and policies: rights-based regulation

Despite progress, accountability to survivors of TF GBV through law and policy remains a challenging area to address. Existing legal frameworks are often insufficient and lag behind rapidly evolving technology and emerging forms of violence. Even though there is growing recognition of TF GBV as a form of discrimination that violates a range of human rights and freedoms, including the rights to access information and participation; to a life free from violence; to freedom of expression; to privacy; and to participate in public and political life, available evidence highlights an important structural gap in accountability mechanisms. There is a high rate of failure by law enforcement to implement appropriate corrective measures to tackle TF GBV (UNFPA, 2021a; The Economist Intelligence Unit, 2021).

> "Advanc[ing] a coordinated global agenda for tackling TF GBV should also involve recognizing that while some countries have the conditions to develop refined legal and institutional models and are able to influence global Internet companies, others struggle to sustain effective judicial and support mechanisms to assist victims."
>
> Jamila Venturini, Executive Director, Derechos Digitales (2022)

The session aimed at exploring rights-based approaches and principles for law and policy to address TF GBV. It built upon the multidisciplinary expertise and experiences of participants with regards to the models, processes, challenges and pitfalls of law and policy. We heard from experts Nina Jankowicz, author

and disinformation expert; Jan Moolman, Association for Progressive Communications; Marcela Hernández Oropa, National Front of Sorority (Mexico); Nighat Dad, Digital Rights Foundation; and Ella Serry, from the eSafety Commissioner of Australia. Five deep discussions with experts followed presentations and plenary discussion.

A multiplicity of approaches to ensure accountability of perpetrators through law and policy are required including independent oversight, self-regulation and public policy.

Nina Jankowicz, author and disinformation expert (see Jankowicz, 2020, 2022), set the stage with a powerful speech entitled, "We are Targets". Jankowicz described her own experience as a survivor of TF GBV after having been appointed as the lead for the Disinformation Governance Board in March 2022, in an effort by the US Department of Homeland Security to counter disinformation. She received an onslaught of online abuse, including doxxing, placing herself and her family at risk of harm.

Jankowicz said the campaign against her "was representative of a larger phenomenon within the American political discourse and the discourse around women, one that makes them an easy target for online abuse".

Her message was a reminder of the entrenched violence and discrimination that women in the spotlight are subjected to, and the broader impact of TF GBV on democracy and gender equality.

Building on the experiences of survivors of TF GBV, Frente Nacional Para La Sororidad (National Sorority Front) successfully advocated for the passing of the first law in Mexico addressing TF GBV, the "Ley Olimpia" (Olimpia Law). **Marcela Hernández Oropa, an activist, expert on digital violence and gender, and a collaborator with the National Front of Sorority and** DefensorasDigitales.org, emphasized the centrality of survivor-led advocacy in the development of this law. The Olimpia Law was advocated for and inspired by the story of Olimpia Coral Melo Cruz, a survivor of image-based sexual abuse. In 2014, when seeking justice for the non-consensual sharing of an intimate video of herself by

an ex-partner, Olimpia discovered that the distribution of such content online was not classified as a crime in Mexico. She successfully advocated for the passing of the Olimpia Law, also known as the Digital Violence Act in all 32 states of Mexico, as well as at the federal level. Passed in 2021, the Olimpia Law defines digital violence and criminalizes the sharing of sexual content without the subject's consent while placing the responsibility on the State to invest in TF GBV prevention. In 2023, the Olimpia Law is being discussed and may soon be approved by the Congresses of Argentina and Ecuador, while feminist movements of survivors of TF GBV in several countries of the Latin American region are advocating to have Olimpia Law in their own countries.

Jan Moolman, co-manager of the Women's Rights Programme at the Association for Progressive Communications (APC), reminded participants that, despite recent progress with the recognition of online GBV as a human rights violation, we are only in the initial stages. She claimed that "laws and policies in the context of rights-based regulation have to go much further". Policy responses should not overprioritize criminalization and punitive measures but must also take a transformative justice approach by focusing on response and remedy for survivors.

> **"Every human seeks pleasure, joy and freedom and the possibility to fully express themselves. These concepts are not considered when [creating] laws and policies. But this is at the heart of responses to TF GBV – TF GBV inhibits the possibility of finding pleasure and freedom in digital spaces."**
> Jan Moolman, APC

Moolman further explained how, as laws and policies continue to be developed and operationalized nationally in consultation with women's activists, "tensions between multiple rights are very present in discussions". In some cases, States have responded to calls for action to address TF GBV with very conservative protectionist measures. These have censored and limited freedom of speech of the same people they were designed to protect, including feminist activists and academics. Measures that protect women and people of diverse sexual orientation and gender identity and expression online

must consider multiple rights, including the rights to safety, movement, participation in public life, freedom of expression and privacy, as well as the rights to bodily autonomy and self-determination. Further, laws and policies also need to consider existing structural inequalities and discrimination that affect how these rights are enjoyed.

Nighat Dad, a Pakistani lawyer and activist, member of the Meta Oversight Board and founder of the Digital Rights Foundation, built on Moolman's points to describe how regulation can be and has been weaponized against women. As Dad explained, TF GBV is the most systemic form of violence on digital platforms, yet governments and organizations alike have been slow to develop appropriate and effective solutions.

> **"[Pakistan] national legislation addressing TF GBV has rarely centred [on] the lived experiences of survivors but focuses instead on carceral models that curb freedom of expression. Legislation ends up criminalizing survivors speaking out about their perpetrators."**
> Nighat Dad, Digital Rights Foundation

According to Dad, the law included ambiguous definitions and gave overwhelming power to law enforcement and regulators who then weaponized it against women themselves. "During the #MeToo movement, the government used the name of national security, morality and social norms to impose violence", Dad denounced.

She stressed the importance of data-driven research and data-based advocacy, survivor-centred policy, and inclusion of local knowledge and cultural context in regulating technology and online spaces. Dad explained that "what some groups or cultures deem as sexually explicit may not align with western notions. For example, the honour killings of Pakistani women for simply having a picture with someone of the opposite sex".

She further suggested that, when faced with the context of authoritarianism and lack of rule of law, communities should explore independent oversight

alongside self-regulation and alternative solutions to hold companies and governments to account.

Lastly, Ella Serry, manager of International Engagement and Capacity Building at eSafety Commissioner, Australia, concluded the presentations with a discussion on government regulation and the role of independent regulatory bodies such as eSafety in comprehensively responding to survivors' needs. She explained that eSafety Commissioner works under a holistic framework with three pillars:

> 1. Protection, through regulatory schemes;
>
> 2. Prevention, through research, awareness-raising programmes, evidence-based education, training and resources for front-line workers and survivors; and
>
> 3. Proactive and systemic change, where they engage with technology companies to focus on Safety by Design, transparency, accountability and responsibility across all products and services to ensure the burden of safety rests with the industry, and not just with users.

eSafety underpins these pillars with a fourth focus on partnerships, in recognition that one single regulator in Australia cannot achieve all these online safety outcomes on their own.

Formed in 2015, eSafety has powers and programmes to address various forms of online and technology-facilitated abuse, which is often gendered and disproportionately impacting marginalized groups, such as LGBTQIA+ Australians, First Nations women, women living with disabilities and linguistically diverse communities. Since early 2022 when an updated Online Safety Act came into force, eSafety's powers have been expanded to address not only image-based abuse, cyberbullying of children and child sexual exploitation material, but also what Australia calls 'adult cyber abuse'. This may include other seriously harmful instances of online violence, such as doxxing or repeated online threats. Serry noted that when directed at women, it tends to be highly gendered, violent and sexualized.

When a complaint is received, eSafety investigates and assesses whether it meets the statutory threshold for action. If it does, eSafety's action could involve reporting abusive content, issuing removal notices to companies and perpetrators, and administering penalties for non-compliance. The objective is to stop abusive content from spreading further online and provide remedy to survivors, who usually just want the harmful content, or their intimate image taken down. eSafety has also established referral pathways with counselling services, including mental health and domestic violence helplines, and provides practical online safety advice and contact details for law enforcement services to survivors.

However, Serry also explained that "this scheme highlights one of the tensions in regulating online harms, which is around balancing free expression and free speech consideration with the need to keep people safe online, free from abuse". In recognition of this, the scheme sets a high bar for adult cyber abuse, with it as needing to be "intended to cause serious, physical or psychological harm, as well as being menacing, harassing or offensive content in all circumstances".

> **Panel discussion:** Ensuring that laws are not weaponized against those they seek to protect
>
> "With the rise of conservatism globally, we are seeing a disciplining of women's bodies across the world today. Further, at the national level, the narrative of women as mothers of the nation State continues to be used to maintain cohesiveness of countries as it has done for generations. At APC, we reflect on the use of language around protection from online GBV. In some cases, these protection measures may turn into increased surveillance and criminalization of sexual speech. In others, anonymity and encryption, which are key enablers of expression, may also limit our ability to trace perpetrators."
> Jan Moolman, APC
>
> "Tensions remain and it's on us to find solutions. One-fits-all approaches will not work as, for example, anonymity is a guarantee for safety for many people in the online space."
> Nighat Dad, Digital Rights Foundation

Participants engaged in further discussions around developing human rights-based and survivor-centred policy and law, as central to ensuring effective regulation. These conversations reiterated the tension between multiple rights and the importance of an equity and justice lens to regulation, both across countries and with a focus on marginalized communities. Key points that arose from the discussion included:

Models and processes

- **Self-regulation versus national law and policy.** The binary between self-regulation and government regulation is an artificial and ineffective division. A combined approach of independent oversight alongside self-regulation and public policy approaches is ideal. Over-regulation and criminalization can serve to prevent survivor reporting and impact upon freedom of expression. However, platforms have too often failed to enforce their own terms of service when it comes to harmful online content. Good business practices, such as independent oversight boards on tech companies and enhanced transparency, need to be coupled with human-rights-based guiding principles to hold companies to account. There also needs to be a higher level of digital literacy among the broader community to ensure that tech companies are held accountable for their own regulations.

- **Protecting freedom of expression.** Understanding what is meant by human rights-based approaches to the regulation of technology companies and social media platforms is central to ensuring essential rights, such as freedom of expression, are protected. However, freedom of expression has too often been co-opted and weaponized by extremist groups to decriminalize and reinforce hate speech and harmful content.

- **Standardization and universal definitions.** Issues of lack of standardized data and contextual adaptation were also brought up in the discussion, evidencing widespread concerns among the TF GBV community. While useful for cross-border enforcement, developing universal definitions is challenging and risks missing important contextual determinants.

Backdoor encryption

- **No backdoor encryption.** Development of a decryption key or tool, for law enforcement or any other accountability mechanism is a double-edged sword that creates an opportunity for bad actors to maliciously attack users. Decryption tools can be easily abused and weaponized against the citizens – women and girls – they are designed to protect. There was full consensus among participants in this breakout session that risks to users' privacy and safety outweigh the potential benefits of this practice. Indeed, it is detrimental in cases of GBV and IPV, where an ex-partner can get access to survivor's private information (also recognizing that law enforcement can be perpetrators), as well as in the case of authoritarian governments, which can use it to exercise censorship and surveillance.

  > "From a security point of view, if there is a backdoor, it would be accessible to all actors, including ill-intentioned ones. In the end, it weakens anonymity for everybody involved. That is why we should look at channels other than decryption, to find the originator of messages and posts."
  > Participant and law professor from India

  Backdoor encryption, while it may be useful in cases of terrorism or public security risks, is not fit for purpose in the case of TF GBV.

- **Metadata as an alternative.** Use of personally unidentifiable metadata could be an alternative to backdoor encryption that protects users' privacy, as long as strong judicial protections are in place to avoid misuse.

Unintended consequences

- **Policies may be weaponized against women and girls.** Early evidence of TF GBV regulations and laws demonstrates that governments may use protection laws to target and silence activists. This leaves TF GBV perpetrators unpunished and further reduces the likelihood that survivors will report cases, and they will endure the ongoing impacts of TF GBV, including offline violence.

- **Global reach versus local laws with respect to content moderation.** Interpretation of defamatory language and what constitutes TF GBV in local settings is often loose, as content moderation requires a deep understanding of the context in which (abusive) content is shared.

- **Data privacy concerns.** Pushing technology companies to proactively report on TF GBV or collect data relating to reporting and incidents, even if well-intended, may cause further harm to survivors, as it is done without their consent and violates their right to privacy.

- **Right-sizing and balancing policy.** Despite potential unintended consequences, there is a need for more innovative TF GBV policies. A balancing act is needed to ensure protection from image-based abuse while not reinforcing heteronormativity and protecting marginalized communities' rights, particularly regarding freedom of expression and sexuality. Further balancing must occur between data privacy and the need for data to inform protective policies, between continuing advocacy and promoting reporting mechanisms, and between acknowledging and respecting consent, legitimacy and confidentiality issues.

Overcoming challenges

- **Survivor-centred response services.** While services to prevent and respond to TF GBV are still being developed in many countries, others lack laws and policies that regulate technology companies and address TF GBV. Given the complexities in which GBV often occurs and the reality of ubiquitous and inadequate judicial responses, one should never assume they know what is best for a survivor. A survivor-centred response is about providing comprehensive options to a survivor so that they decide what is best for them. However, effective policies and practices that remove the onus of responsibility to seek justice from survivors and place it on technology companies and response services are required. A participant and executive director of a United States CSO, explained how processes to obtain proof of abuse from tech companies (i.e. in the form of metadata) are time-consuming since these data are not considered to be owned by users/survivors. She also described how police officers often revictimize survivors by asking them to provide such proof of abuse. A participant from a Uganda CSO described outright victim-blaming by officers in cases of image-based abuse.

- **Tech platforms and companies must invest in safety.** There are several actions that tech companies and social media platforms could take to ensure technology and online spaces are safe. These include establishing effective reporting mechanisms for TF GBV and mechanisms to ensure privacy and data ownership for survivors, building relationships with CSOs and holding consultations with them, as well as users, to review reporting tools, and investing in content moderation and the well-being and safety of human moderators. Companies could also invest in strengthening existing GBV response mechanisms to integrate and address TF GBV.

- **Cultural and local context in content moderation.** The bias in human content moderation and the diverse cultural understandings of abuse may lead to suboptimal responses to abusive content complaints. Further, if content moderation policies are centrally created, these do not reflect contextual values and perspectives on ethics and what constitutes GBV. Understanding local perspectives is central to creating and enforcing content moderation policies suitable for every context.

Accountability

- **Survivor-centred and contextualized legislation.** Policy and legislation must be designed in close consultation with women and girls, survivor advocates and front-line services providers. It must be both survivor-led and survivor-centred. Further, the language of law and policy must be carefully crafted and framed contextually to hold those that perpetuate TF GBV to account, while being diligent to avoid victim-blaming.

  > "[There is no offence of] image-based abuse [in India. Indeed, the] laws penalize obscenity. Obviously, that is not survivor-centred and plays into the patriarchal view [of ownership over women's bodies] and does not provide help to the survivor. The framework and the language is vital. Again 'obscenity' punishment is an example of dangerous language in law."
  > Participant and lawyer from a CSO

- **Global, cross-border action.** Participants highlighted the value of partnerships, coordination and agreements to address TF GBV. Consensus was reached around the need for regional and global standards and accountability mechanisms to address TF GBV, following a similar model to the European General Data Protection Regulation. This model would set the benchmark for regulation and enable and enforce compliance across business and tech, regardless of jurisdictional complexities. Indeed,

"...if [tech companies] have this infrastructure, [they should] apply it everywhere else".[7]

- **Partnerships and networks play a key role in coordination, particularly among regulators.** The Global Online Safety Regulators Network, for example, is a recently established network fostering partnerships between regulators (including across the United Kingdom, Europe, Asia and the Pacific) to facilitate cross-border enforcement and accountability.

- **Technology companies to be held accountable.** No one mechanism is sufficient to ensure accountability for preventing and responding to TF GBV. A range of different mechanisms to hold technology companies accountable for the abuse that is perpetrated and amplified on their platforms must be explored and implemented. Accountability should be enforced through laws that not only target content moderation, but also focus on reporting mechanisms for survivors and address the algorithms that spread the abuse. Further, technology companies should bear the responsibility of continually updating safety practices and procedures. They must be transparent about the abuse and TF GBV that takes place and how it is being addressed. There is power in enforcing transparency through public pressure, "[tech companies] would be more inclined to invest in solutions to protect themselves if they were getting that feedback publicly".[8] Furthermore, organizations, including

---

7 Participant and data scientist from a large government aid organization.

8 Participant and lawyer from a large technology company

front-line service providers and survivor advocate groups must be supported with the digital literacy to hold the tech companies to account for their own self-regulatory policies.

- **Need for training and education.** To ensure effective enforcement of law and policy, whole government approaches must be taken. It is vital to build and strengthen the capacity of regulators, decision makers, law enforcement actors and the judiciary to receive, investigate and respond to cases of TF GBV in a timely, comprehensive and survivor-centred manner. Training must be delivered on an ongoing basis and focused on providing survivor-centred and trauma-informed services, as well as on emerging technologies and digital tools and spaces. Legal systems must also be equipped with resources to ensure no harm is perpetrated against survivors who are seeking justice.

Key takeaways

1. Approaches and beliefs differ around freedom of expression, privacy and criminalization; therefore, human-centred and survivor-centred approaches and perspectives are necessary to ensure policy and regulation are not doing more harm.

2. A combination of self-imposed policies by technology companies, government regulation, community regulation, and global and regional frameworks and partnerships are necessary to prevent and end TF GBV globally.

3. Centring on human rights within policy rather than specific acts or definitions of TF GBV minimizes the weaponization of regulation against activists and is more future-proof.

4. Alternative solutions, such as metadata, should be explored in place of backdoor encryption. The existence of decryption keys or tools which create opportunities for bad actors to attack users and risks to survivor safety outweigh the potential benefit.

5. Context matters – human-rights-based and survivor-centred approaches are needed to ensure regulation is not weaponized against survivors or activists and does not violate privacy or freedom of speech.

6. The problem must be recentred on what survivors need rather than on what policymakers think women and girls need or what is convenient to implement.

7. Increased digital literacy is necessary for policymakers and regulators to address TF GBV, particularly in emerging technologies.

8. Laws and policies must be developed in partnership with survivor advocate organizations, feminist technologists and lawyer groups.

9. There is a need for global and cross-border regulations and partnerships, accounting for contextual and cultural specificities that reflect the experiences of TF GBV and help-seeking behaviours.

Recommendations

Given the constantly evolving forms and specific characteristics of TF GBV, prevention, mitigation and response efforts require the collective efforts of donors, policymakers, governments, researchers and academics and technology companies.

The following recommendations result from expert discussions from the first global symposium on TF GBV. These have been informed by background research papers and diverse experts from CSOs, academics, multilateral organizations, technology companies and policymakers.

All our work must be guided by approaches based on human rights, taking account of the experiences of women and girls in all their diversity to ensure that prevention and response to TF GBV is meeting their needs.

Donors:

- Do not ask for excess data – only ask for the minimum required data.

- Clearly identify information needs prior to asking fundees to collect data.

- Fund local organizations and research groups.

- Look holistically at what a survivor needs.

- Do not fund unethical technology or data collection.

- Carefully review the data collection methodology, management and use and assess risk to survivors and advocates. Ensure that risks do not outweigh potential benefits.

- Understand that collecting any GBV data increases the risk of harm to the survivor and those around them.

- Invest in and require data stewardship for all employees with access to data, internally and for all receiving organizations.

- Encourage deep contextual understanding of TF GBV at a local level, if not directly funding a local organization.

- Do not assume that because a programme or response worked in one context, it will work in all other contexts – GBV and TF GBV are context dependent.

- Invest in digital literacy, especially within women's organizations and for GBV front-line responders.

- Require all grantees to follow global GBV data ethics guidelines for GBV and TF GBV.

- Do not fund extractive data collection. Fund local research with a well-established presence that will ensure the results are locally useful.

- Fund holistic response programmes grounded in GBV response.

- Fund safe and ethical technology for GBV programming to prevent TF GBV.

- Discourage the collection of unnecessary GBV and TF GBV data and act upon existing research.

- Require fundees to gain informed, authentic and ongoing consent from data subjects.

- Encourage diverse collaboration across sectors and industries but ground the work in GBV normative frameworks and feminist theory.

Policymakers:

- Create policies based on local context and nuanced understanding of TF GBV.

- Do not focus too much on specific elements of TF GBV, since they will likely change by the time policy is implemented, instead focus on human rights and survivor-centred approaches.

- Do not only focus on criminalization; instead understand the holistic needs of survivors.

- Encourage strong data stewardship.

- Do not allow backdoors for encryption.

- Create policy that understands and encourages abidance of global GBV data ethics guidelines by State and non-state actors.

- Minimize the weaponization of regulation against activists and make it more future-proof by centring on human rights within policy rather than on specific acts or definitions of TF GBV.

- Context matters – human rights-based and survivor-centred approaches are necessary to ensure regulation is not weaponized against survivors or activists and is not violating privacy or freedom of speech.

- Laws and policies must be developed in partnership with survivor advocate organizations, feminist technologists and lawyer groups.

- Consider technology company regulation that finances the response to TF GBV.

Government:

- Create and fund holistic survivor-centred approaches when responding to TF GBV.

- Encourage strong data stewardship.

- Explore alternative options to backdoor encryption that protects users agency and privacy.

- Encourage all of government to understand, respect and follow global GBV data ethics guidelines for GBV and TF GBV.

- Discourage the collection of unnecessary global GBV data and act upon existing research.9

- A combination of self-imposed policy by technology companies, government regulation, independent oversight, community regulation, as well as global and regional frameworks and partnerships are necessary to prevent and end TF GBV globally.

- Global and cross-border regulations and partnerships are needed, while accounting for contextual and cultural specificities which reflect the experiences of TF GBV survivors and their help-seeking behaviours.

- Increase funding of TF GBV solutions that are grounded in existing GBV response services.

---

9   GBV is pervasive in all contexts. Nearly one in three women globally have experienced GBV at least once in their lifetime (Violence against women prevalence estimates, 2018, World Health Organization; 2021).

Researchers/academics:

- Ground TF GBV research methods in global GBV data ethics guidelines.

- Risk of harm to survivors cannot outweigh the purpose and need for data and research. TF GBV data collection should not take place unless participants' safety can be ensured, specifically there must be TF GBV response services established.

- Be extra vigilant when dealing with TF GBV data, especially if creating data sets of survivors data.

- Do not use data that has been collected unethically.

- Understand that data collected is part of the person from whom it was collected and not something a researcher, organization or company can own.

- Do not replicate extractive practices from technology companies or past research models.

- Have strong data stewardship.

- Do not make global prevalence claims without local contextual understanding, especially since TF GBV can be nuanced and situational yet extremely damaging and harmful.

- Consent gained by data subjects should be informed, authentic and ongoing, not a one-time interaction.

- Do no harm, survivor-centred, intersectional and participatory research processes must be considered across all steps of the research/data process: from defining needs to data collection, analysis and dissemination.

Technology companies:

- Value the experiences of women and girls – not only to avoid harm but to understand their needs and build the technology they need.

- Build business models on positive interactions – rather than being content agnostic.

- Create multidisciplinary teams and partnerships and include GBV experts when creating GBV solutions or policies.

- Do not practice extractive behaviour, including data collection.

- Encourage strong data stewardship.

- Understand and embed global GBV data ethics guidelines into company policies and practices.

- Understand that data collected is part of the person from whom it was collected and not something a researcher, organization or company can own.

- Consent gained by users and data subjects should be informed, authentic and ongoing, not a one-time interaction.

- Innovative approaches and ideas, grounded in offline GBV normative frameworks and expertise, are necessary to ensure the proper safety of women and girls in the digital age.

References

Apple Support (2022, September 27). How safety check on iPhone works to keep you safe. Cupertino, CA: Apple Inc. https://support.apple.com/guide/personal-safety/how-safety-check-works-ips2aad835e1/web

Association for Progressive Communications (2022). *Women's Rights Programme*. Available at: www.apc.org/en/wrp

Callisto (2023). Callisto Vault. Available at:. www.projectcallisto.org/documentmatch

Centers for Disease Control and Prevention (CDC) (2020, September 17). *Infographic: 6 guiding principles to a trauma-informed approach*. Available at: www.cdc.gov/cpr/infographics/6_principles_trauma_info.htm#:~:text=Participants%20learned%20SAMHSA%E2%80%99s%20six%20principles%20that%20guide%20a,%26%20choice%206%20Cultural%2C%20historical%20%26%20gender%20issues

Chayn https://www.chayn.co/

Chayn (n.d.). Orbits: a global field guide to advance intersectional, survivor-centred, and trauma-informed interventions to TGBV. Available at: https://chayn.notion.site/Orbits-a-global-field-guide-to-advance-intersectional-survivor-centred-and-trauma-informed-interv-8d8dc6a1436543b8b25af63ddafaa409

Clinic to End Tech Abuse (CETA) www.ceta.tech.cornell.edu/

Digital Rights Foundation https://digitalrightsfoundation.pk/

Dunn, S., Vaillancourt, T., Brittain, H. (2023, June 8). *Supporting Safer Digital Spaces.* CIGI: Waterloo, ON, Canada. Available at: www.cigionline.org/publications/supporting-safer-digital-spaces/

eSafety Commissioner. *Safety by Design*. Canberra: Government of Australia. Available at: www.esafety.gov.au/industry/safety-by-design

Gender-Based Violence Information Management System (GBVIMS) www.gbvims.com/

Hinson, L. (2022). *Technology-facilitated gender-based violence. Data and measurement: Methodology matters.* New York: UNFPA. Available at: www.unfpa.org/resources/technology-facilitated-gender-based-violence-data-and-measurement

Hussain, H. (2021, May 23). *Trauma-informed design: Understanding trauma and healing. Designing interfaces, narratives and services that uplift.* San Francisco, CA: Medium. https://blog.chayn.co/trauma-informed-design-understanding-trauma-and-healing-f289d281495c

Hussain, H. (2022) *Technology-facilitated gender-based violence. Business and technology: feminist design.* New York: UNFPA. Available at: www.unfpa.org/resources/technology-facilitated-gender-based-violence-feminist-design

International Rescue Committee (IRC) https://www.rescue.org/

Jankowicz, N. (2020). *How to lose the information war: Russia, fake news, and the future of conflict.* Washington, DC: Wilson Center. www.wilsoncenter.org/book/how-lose-information-war-russia-fake-news-and-future-conflict

Jankowicz, N. (2022). *How to Be a Woman Online: Surviving Abuse and Harassment, and How to Fight Back.* London: Bloomsbury Academic.

Lo, K. (2020, November 18). *Toolkit for Civil Society and Moderation Inventory.* San Francisco, CA: Meedan. https://meedan.com/post/toolkit-for-civil-society-and-moderation-inventory

Meedan https://meedan.com/

Office of the Spokesperson (2022, March 16). *2022 Roadmap for the Global Partnership for Action on Gender-Based Online Harassment and Abuse.* Washington, DC: US Department of State. Available

at: www.state.gov/2022-roadmap-for-the-global-partnership-for-action-on-gender-based-online-harassment-and-abuse/

Plan International (2020). *Free to Be Online?* Woking, UK: Plan International. https://plan-international.org/publications/free-to-be-online/

Pollicy https://pollicy.org/

SmartNoise https://smartnoise.org/

Tattle https://tattle.co.in/

The Economist Intelligence Unit (2021, March 1). Measuring the prevalence of online violence against women. Available at: https://onlineviolencewomen.eiu.com/

Uli https://uli.tattle.co.in/

UNFPA (n.d.) *Bodyright.* Available at: https://www.unfpa.org/bodyright

UNFPA (2021a, December 1). *Technology-facilitated gender-based violence: making all spaces safe*. Available at: www.unfpa.org/publications/technology-facilitated-gender-based-violence-making-all-spaces-safe

UNFPA (2021b). *Strategic Plan 2022–2025*. Available at: www.unfpa.org/strategic-plan-2022

UNFPA (forthcoming). Flourish: GBV Operational Plan. New York.

Venturini, J. (2022) Technology-facilitated gender-based violence. Law and policy: Rights-based regulation. New York: UNFPA. Available at: www.unfpa.org/resources/technology-facilitated-gender-based-violence-rights-based-regulation

Wilson Center *Accessing Justice: Gender-Based Violence and the Rule of Law.* Available at: https://gbv.wilsoncenter.org/

Wilson Center. *Science and Technology Innovation Program*. Available at: www.wilsoncenter.org/program/science-and-technology-innovation-program

World Health Organization (2021, March 9). Violence against women prevalence estimates, 2018. Available at: https://www.who.int/publications/i/item/9789240022256