November 2022

Author

Hera Hussain, is the Founder and CEO of CHAYN - a global, survivor-led nonprofit that creates multilingual resources on the web to support the healing of survivors of gender-based violence. Hera is an Ashoka Fellow, and was on the Forbes 30 Under 30, MIT Technology Review's Innovators Under 35 and European Young Leader 2020 list.

Business and Technology: Feminist Design

Overview: This document presents the summaries of ten seminal resources related to business and technology's interaction with technology-facilitated gender-based violence (TFGBV), defining how current practices are unsafe for women, marginalized communities and survivors, and a feminist approach to rethinking design and cyber security. The purpose of the upcoming discussion is to build consensus on best practices for ethically engaging and dismantling the systems incorporated in business practices and technological design that perpetuate TFGBV.

Women have been at the forefront of developing technology, but over the years, gendered power imbalance and skewed business models have systemically edged out women and feminist design participation. As everyday technology use becomes the norm, the harm posed and perpetuated by technology designed for the "default male" user deepens.[1] This is further exacerbated by increasingly common technology such as artificial intelligence (AI), deepfakes, stalkerware, and internet-of-things (IoT).

1. "Default male" is a term used in Caroline Criado Perez's book Invisible Women: Data Bias in a World Designed for Men where she shows that much of our daily life is designed by and for males and men because females and women are either not considered at all or considered "just too complicated". A couple examples include, heart attack symptoms, seatbelts, medications, and technology.

Photo: © Mbuto Machili for UNFPA Mozambique

Lack of diversity of product teams and leadership, as well as a lack of prioritisation of the increased harm faced by women and marginalised genders, and those that find themselves at the intersections of multiple oppressions, has resulted in products, policies, and services that are unsafe and put survivors of gender-based violence (GBV) at risk. In many cases, the technology itself is a cause of trauma or re-traumatisation despite repeated claims that "technology is neutral and it's how people use it" which dismisses the issue as a sociological or user based problem. One clear example, included in this review, of how harms to women have been ignored is shown in Slupska's research on IoT "smart" home security devices. Her research shows that out of 40 cybersecurity papers reviewed, only one article mentions domestic violence, a harm that largely affects women. This absence of women or feminist approaches to cybersecurity cuts across all technology and is highly problematic for the safety of women and marginalised groups.

Despite the increasing coverage of technology-facilitated gender-based violence (TF GBV) in media, public policy and academia, the market prioritisation and business incentives have changed little. There is however, a growing resistance to this approach by technologists, activists and academics who are working to create survivor-centred frameworks and solutions to addressing/mitigating/preventing TF GBV.

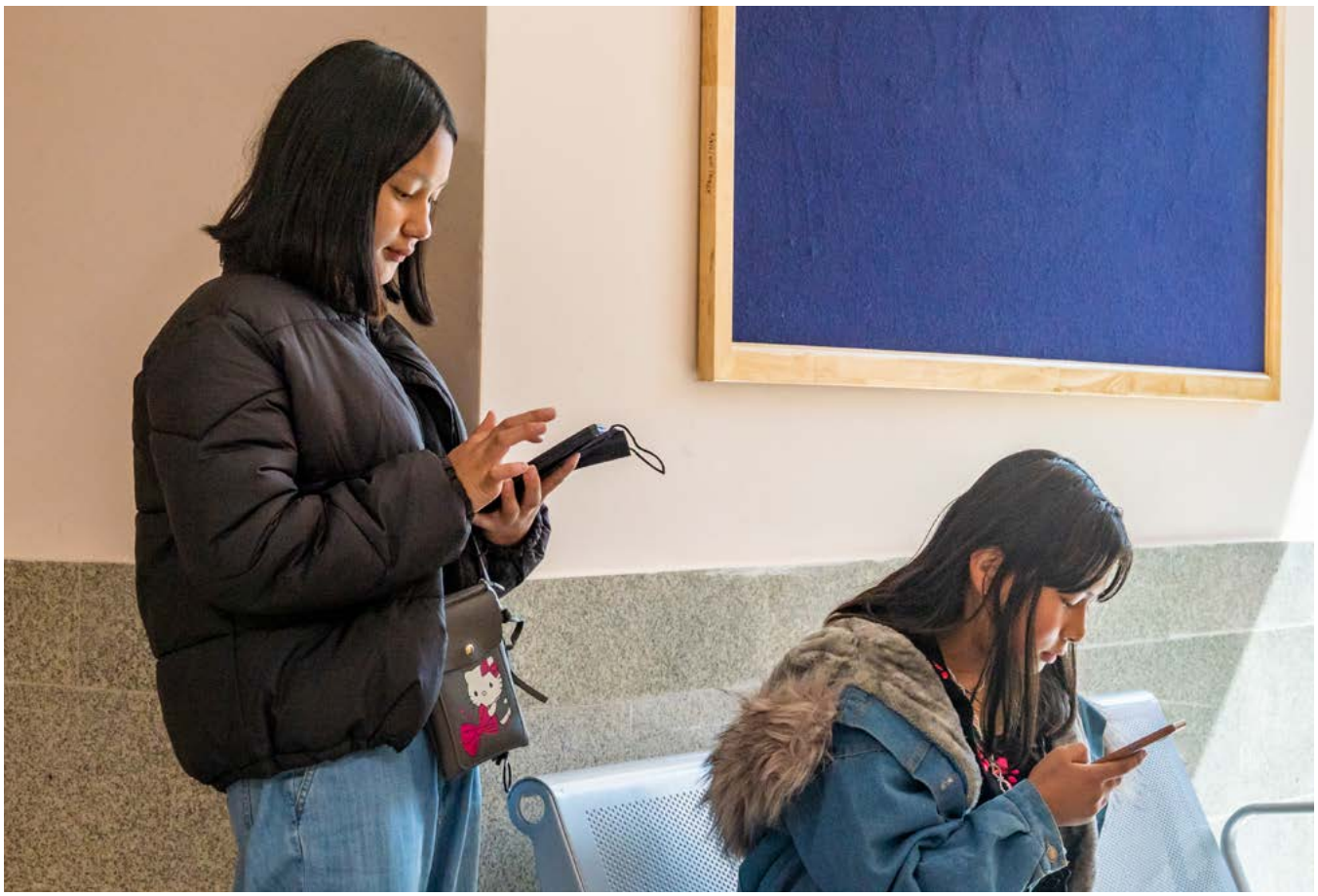

Photo: © UNFPA APRO

Summary of Background Papers

Trauma-informed design to tackle technology-facilitated gender-based violence, 2022 Chayn

Summary: The trauma-informed design principles were created by Chayn based on their work on gender-based violence, especially tech abuse. These were applied and further crafted through the Orbits project where Chayn and End Cyber Abuse, consulted technologists, activists, survivors, academics and designers globally on the principles and how they can be applied to technology-facilitated abuse.

Design principle	Application
Safety Making brave and bold choices that prioritise the physical and emotional safety of people.	• 2 Factor Authentication • Sharing last known logins and locations • Permitting third party reporting (with informed consent from survivor) • Reporting to platforms for offline behaviour of users • Safety exit button on websites. To support emotional safety, consider redirecting to something comforting instead • Allowing users to opt for disguised emails with fake subject lines, like Chayn's mini-course platform Soul Medicine • Blocking and filtering content and users
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.	• Allowing people to access essential information without having to create accounts • Giving an option of what information is kept public and private, such as full names and location • Actively asking survivors for their consent in sharing information with other agencies and individuals within the organisation, and being clear with survivors about how and why their information is being shared.
Equity Designing for inclusion must consider how position, identity, vulnerabilities, experiences, knowledge, and skills shape trauma and recovery. Survivors are not a homogenous group.	• Designing products that cater to a range of accessibility requirements such as speech and hearing impairments • Providing resources and information in multiple formats - for example, captioned videos as well as written resources • Ensuring strong referral pathways to specialist services for survivors from marginalised communities • Rolling out new safety features simultaneously in all low and high-income countries and enable reporting in multiple languages • Providing staff training and learning opportunities on anti-oppression and decolonisation

Design principle	Application
Privacy Securing a survivor's personal information, such as data, images, videos, statements, and their trauma story must be kept secure and undisclosed, unless the survivor decides otherwise. Also ensuring frictionless access to help and information.	• Clearly indicating what data is publicly accessible and what isn't • Automatic disabling of cookies and tracking when survivors report abuse on platforms • Using end-to-end encrypted technology and exploring the use of privacy-enhancing technologies (PET) such as encryption and data masking • Withholding survivors' details with the perpetrator during any punitive actions taken • Providing survivors with a digital file of evidence that can support civil and criminal cases, if they want to pursue those routes
Accountability Maintaining a relationship of trust includes being open and consistent about what is being done, how, and why; we must create and nourish constructive feedback loops that trigger change	• Providing clear ways to help survivors identify in-platform reporting mechanisms such as quick access bars for reporting abuse • Acknowledging gaps in knowledge or foresight which can contribute to harmful features • Being consistent and predictable in product design - by providing structure and routine • Committing to long-term systemic change, rather than reacting to scandals and infrequent public outrage
Plurality Actively leaving space for complexity and recognising harm manifests in different and disproportionate ways for people living at the intersection of multiple oppression.	• Training moderators to understand cultural context • Refraining from assuming which language is spoken based on location • Offering ways for people to customise their journey on product • Training staff on the impact of additional vulnerabilities, such as caste, race, religion, sexual orientation, and disabilities • In complaint processes, it should be possible for survivors to identify multiple offences, including offline ones
Power sharing Distributing and sharing power by co-designing interventions with survivors.	• Giving survivors decision-making power in tech companies through compensated board or committee positions (only with survivors informed consent and respect for their confidentiality) • For global firms, using local teams and networks to gather ideas for ways to improve services across the globe • Creating community-owned models and practices for governance and evaluation • Translating and localising content and policies
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.	• Using an empathetic tone in written and vocal communications • Ensuring visual assets are not retraumatizing. Displaying simple, soothing, and visually appealing user-experience (UX). • Prioritising ethical considerations in corporate decision-making over shareholder priorities • Providing realistic information about reporting processes. (For example: 'we respond to requests in 2 to 48 hours, with 70% of reports getting an answer within 10 hours') • Taking proactive and communicative steps to stop tech abuse (For example: flag and/or blur offensive content and create digital fingerprints to block uploading of flagged content)

The full report can be seen here.

Datasheets for Datasets, 2018 Timnit Gebru, Jamie Morgenstern, Briana Vecchione, Jennifer Wortman Vaughan, Hanna Wallach, Hal Daumé III, Kate Crawford

Summary: This report seeks to address AI bias by creating a systematic method of documenting the creation and use of datasets, specifically used with machine learning. The researchers "propose that every dataset be accompanied with a datasheet that documents its motivation, composition, collection process [and] recommended uses". If there is a standardised process for documenting machine learning datasets, then it will be easier to understand when bias is occurring and how to mitigate it.

The datasheet consists of seven sections: motivation, composition, collection process, preprocessing/ cleaning/ labelling, uses, distribution, and maintenance. Each section includes between 4 and 12 questions to be answered by the dataset creator. The end result is a report about the dataset.

The full report can be seen here.

Follow up work on documenting machine learning models can be found in Model Cards for Model Reporting.

Trauma-Informed Computing: Towards Safer Technology Experiences for All, 2022 Janet X. Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, Nicola Dell

Summary: Researchers used the following listed principles of trauma-informed care and adapted them to four areas of computing research and practice: user experience research & design, security & privacy, artificial intelligence & machine learning, and organisational culture in tech companies.

- **Safety:** Ensuring that people feel safe when using, designing, or otherwise interacting with technology, physically and emotionally.
- **Trust:** Ensuring technology artefacts, processes and organisations operate transparently, predictably, and reliably while providing users with the ability to make mistakes and corrections.
- **Peer Support:** Ensuring that online peer support is non-judgmental, empathetic, and respectful.
- **Collaboration:** Ensuring interfaces and user interactions with a platform are collaborative rather than autocratic and involves the broader ecosystem; and survivors have input during the development and evaluation of new technologies.
- **Enablement:** Ensuring design decisions have positive impact on individuals and communities and changes are made to give people greater control over their decisions and well-being.
- **Intersectionality:** Developed through lineages of Black feminist scholarship, consider how power relations at different levels of social structure are intertwined and mutually constructed.

The following table covers some applications of the principles of trauma-informed care.

Area	Topic	Example Good Practice
UX Research & Design	User Research User Interface Design Usability Assessment	• Carefully consider how user research can be retraumatizing and work to minimize potential harm. ["seek ways to avoid retraumatization"] • Conduct user studies in a place where participant feel safe and familiar [safety, trust] • Consider involving survivors in the research process [collaboration, enablement] • Draw inspiration inspiration from trauma-informed design principles in other environments such as physical spaces [saftey, trust] • Create, publish, and encourage reuse of trauma-informed design patterns [trust, collaboration] • Evaluate how technology or interface may traumatize or retraumatize its users *["seek ways to avoid retraumatization"]*
Security & Privacy	Threat modeling Indicators & settings	• Include "causing psychological distress" as a common adversarial goal *["acknowledge trauma and its impact"]* • Work with survivors to surface adversarial goals and capabilities [collaboration] • For software updates, provide clear information that warns users ahead of time on any upcoming changes, with options for whether and when to update [safety, trust] • For security warnings, reflect on the impacts of established "best practices" (e.g., using harsh colors and forcing attention) on hypervigilant users *["seek ways to avoid retraumatization"]*
Artificial Intelligence & Machine Learning	Automated social decisions Recommender systems Content moderation & filtering Intelligent agents	• Audit algorithms and datasets in systems that make socially consequential decisions (e.g., in criminal justice, employment) [trust, collaboration, intersectionality] • Clearly explain why a particular recommendation shows up (e.g., a GPS system ad is a result of search histories, not an indicator of being stalked) [trust] • Let users disallow certain ad toppics across different websites and platforms [collaboration, enablement] • Be attuned to how automatic flagging can inadvertently remove benign content importatn to marginalized communities [intersectionality] • Create content policies with input from impacted communities [collaboration] • Ensure agents do not judge users or increase users' anxieties [safety, trust] • Build agents that empathetically respond to intersectional issues [intersectionality]
Safety	Work processes Workplace culture	• Provide training & resources to help workers better interact with trauma survivors and process secondary trauma [safety, peer support, enablement] • Provide accommodations for employees to flexibly manage their schedules, workload, and exposure to traumatic content [collaboration, enablement] • Ensure that workplace policies account for empoyees experiencing traumatic events (e.g., death, illness, racism) [*"acknowledge trauma and its impact,"* intersectionality] • Ensure that internal processes for handling harassment and discrimination cases hold perpetrators accountable and enable survivors to heal [safety, trust, intersectionality]

Read more here.

Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things, 2021 Julia Slupska and Leonie Maria Tanczer

Summary: Current cybersecurity literature is almost entirely blind to intimate partner violence (IPV). This paper seeks to create a "socio-technical" approach to address this gap using the emerging field of Internet of Things (IoT) or "smart" devices as an example.

Researchers looked at the risks and harms posed to victims/survivors from many "smart" devices such as conventional household appliances connected to the internet. The interdependencies between different products and the devices' enhanced functionalities create risk for coercion and control.

They applied the method of "threat modeling," a common technique used in cybersecurity and shifted the conventional technical focus from the risks to systems toward risks to people.

Tech Abuse Threat Model	
Ownership-based compromise	Being the Owner of a device or account allows a perpetrator to prohibit victims'/ survivors' usage or track their location and actions
Account/device compromise	Guessing or coercing credentials which enables a perpetrator to install spyware, monitor the victim/survivor, steal their data, or lock them out of their account
Harmful messages	Contacting victims/survivors or their friends, family, employers, etc. without their consent
Exposure of information	Posting or threatening to post private information or nonconsensual pornography (i.e., image-based sexual abuse
Gaslighting	Using a device's functionality (e.g., remote changing of temperature) to make a victim/ survivor feel as if they are losing their sanity and/or control over their home.

By using a smart lock system as a case study, they present a model for technology companies to identify IPV threats and create design changes that reduce the likelihood of harm based on the threat model. The following is a table of mitigative strategies.

Ownership-based compromise	**Restricting ownership:** Company having a protocol which allows them to remove owner access when abused (e.g domestic abuse)
	Equalising account holder rights: Multiple account owners, allowing distribution of power.
	Consent changes: Shared devices should require all associated users to consent to fundamental changes.
	Customer-facing staff guidance: Supporting staff to identify how to assist users in instances of disputes around who is a legitimate account holder.
Smartphone compromise	**Automatic logouts:** Periodic logging out of users from accounts, prompting re-authentication when using a smartphone to lock/unlock smart locks.
	Report-theft feature: A web-based feature to report theft or takeover of devices.
Account compromise	**Register of login details:** Vague, innocuous-looking regular notifications of login locations and timestamps.
	New login prompts: Notifications to an account whenever an IoT device login is attempted.
	Change of password prompts: Requirement of new login across all devices if a user changes password.
	Reinstate account ownership: Reinstate access to compromised accounts through time-stamped backups so survivors can access and control their data.
	Multi-factor authentication: Multi-authentication methods so accounts are less vulnerable to password coercion.
	Transparency around privileges: Users on lower authorization levels should receive frequent reminders of the different access & power other Accounts have.
	Access trials: Notification to all users of account holders checking critical settings such as access logs.
Smart lock compromise	**Factory reset:** Simple activation from inside home Wi-Fi network to reset a IoT device to its original state, enabling survivors to restrict access after a threat.
	Logs: Access logs (who, when, where) should not be subject to changes and edits.
	Disable functionalities: Users should be able to disable functionalities e.g remote closing/ unlocking of a door.
System compromise	**Connection reminders:** Regular reminders of which IoT devices are connected and which user accounts have access to them.
	Opt-out: Allowing opt-out of certain data collection which aren't essential to the functionality.
	Actionable advice: Tailored company guidance for survivors on steps to follow if they are facing domestic abuse or harassment.

Read more here.

No Excuse for Abuse, PEN America

Summary: PEN America's report presents a mix of proactive, reactive and accountability measures to tackle online abuse. Recommendations are from the experiences and needs of writers and journalists who identify as women, BIPOC, LGBTQIA+, and as members of religious or ethnic minorities.

Empowering Targeted Users And Their Allies	
Proactive Measures: Reducing Risk And Exposure	• Allowing proactive filtering of content by users and their allies • Enhanced safety modes and visibility snapshots • Delegate account access to trusted allies
Reactive Measures: Facilitating Response And Alleviating Harm	• Access to emergency support from the platform • Features to automate quick documentation of abuse • Improve blocking, muting and restricting engagement and content from abusers • Make reporting user-friendly and trauma-informed by ensuring clarity, consistency and allow bulk reporting • Support third-party tools designed to counter online abuse—especially those built by and for women, BIPOC, and LGBTQIA+ technologists

Disarming Abusive Users	
Accountability Measure	• Make rules and repercussions clear and easily accessible in real time from directly within the main website • Establish a transparent system of escalating penalties for abuse including warnings, strikes, temporary functionality limitations, suspensions, content takedowns and account bans. • Proactive nudges to encourage users to rethink abusive content before they post it. • Improve the appeals process for users subjected to content or accounts taken downs, restriction, or suspensions.

Further feminist technology frameworks

Data Feminism, by Catherine D'Ignazio and Lauren Klein

Summary: Data feminism presents 7 principles for how data science, and data scientists can be used for good and not participate and perpetuate systems of oppression.

1. **Examine power.** Data feminism begins by analyzing how power operates in the world.
2. **Challenge power.** Data feminism commits to challenging unequal power structures and working toward justice.
3. **Elevate emotion and embodiment.** Data feminism teaches us to value multiple forms of knowledge, including the knowledge that comes from people as living, feeling bodies in the world.
4. **Rethink binaries and hierarchies.** Data feminism requires us to challenge the gender binary, along with other systems of counting and classification that perpetuate oppression.
5. **Embrace pluralism.** Data feminism insists that the most complete knowledge comes from synthesizing multiple perspectives, with priority given to local, Indigenous, and experiential ways of knowing.
6. **Consider context.** Data feminism asserts that data are not neutral or objective. They are the products of unequal social relations, and this context is essential for conducting accurate, ethical analysis.
7. **Make labor visible.** The work of data science, like all work in the world, is the work of many hands. Data feminism makes this labor visible so that it can be recognized and valued.

Photo: © UNFPA Myanmar

Consentful Tech

Summary: The FRIES (Freely given; Reversible; Informed; Enthusiastic; Specific) model became an accessible way to talk to young people about bodily autonomy and consent. It goes beyond "No means no" which, while powerful, doesn't offer an alternative to what consent can look like. The Consentful tech project proposes we use this framework and apply it to technology design as well.

Trust and Abusability Toolkit, Angelika Strohmayer, Julia Slupska, Rosanna Bellini, Gina Neff, Lynne Coventry, Tara Hairston, Adam Dodge

Summary:
This toolkit is a collection of resources which includes the following:

- Recommendations for gender-based violence advocates in supporting survivors of technology-mediated abuse and for engaging with technology companies to improve their services
- Advice for technology companies and researchers wanting to implement safety features that better support survivors and proactively engaging with perpetrators
- Abusability and the secure systems development life cycle provides an outline for a development life cycle that takes peoples' safety into consideration
- A self-evaluation tool for technology companies of how mature their features are in relation to the safety

Analysis of Background Papers

As displayed by this review of work, there's a great deal of consensus and agreement on the need for survivor-centered technology design and using feminist theory to support a new approach.

From all the factors the papers agree on, these ones are notable.

- **Technology is not neutral.** There's an agreement that technology itself is not neutral and gaps in inclusive design (such as a "smart" lock) can lead to restricting privacy and facilitating coercive and controlling behaviours. This is a significant consensus because the prevalent narrative in the technology sector is still that technology is not the problem: the problem rests with abusive users.
- **We need an end-to-end, multi-factor response for the entire ecosystem.** Any gender-based violence lens needs an end-to-end approach that requires all stakeholders to participate. This involves companies to safely and ethically co-design with and for survivors, work alongside advocates and law enforcement to document and provide policies that support the healing of survivors and hold abusers accountable.
- **Consent, safety, intersectionality and survivor-centred** are the most common principles shared across all ethical and feminist frameworks. Consent cannot be a one-time legal compliance check, but must be integrated throughout our technology. Safety by design is defined as physical and psychological safety which is a more holistic concept than only considering threats to the body. Intersectionality is referred to by different words and phrases but all acknowledge how people at the intersections of different oppressions will experience harm differently and this will need to be considered across all aspects of product life cycles, Survivor-centred design and intervention is specially highlighted across all papers. Users are critical to their own healing and should be central in how harm to them could be reduced or mitigated.
- **Harm can be reduced but cannot be eliminated.** There is consensus that tech abuse is both a technological and social problem and that interventions must address both in order to address the issue.
- **Principles of trauma-informed care create an alternative approach to technology-design.** SAMHSA's established and widely consulted principles of safety, trust, collaboration, peer support, enablement, and intersectionality for in-person care can be used for technology design. It can teach us about the non-linear, individual and collective nature of trauma, and how healing support should be structured. Most of these principles are explicitly mentioned or are described in similar ways.
- **No technology will be inclusive if it doesn't learn and apply learning from social and racial justice, feminist theory, and post and de-colonial movements.**
- **Trauma-informed approaches for survivors would make platforms safer for everyone.** Instead of thinking of the extra considerations as a burden, platforms should understand implementation would create a better and safer experience for all users.
- **Feminist technology is not a check-list but an ongoing commitment to improving design processes and outcomes.**

Where scholarship diverges

There are very few points of divergence in these papers which could signal that the feminist technology sector is both small, and arising as a response to issues identified from grassroots movements. The differences arise out of the expertise of the authors and the "lens" they employ in examining tech abuse.

- Most papers depict domestic and sexual violence within family or intimate settings. With the growing concern around incel communities, there is a critical need to also consider how to address the risks of coordinated group attacks that are gender or identity motivated.
- While the literature does highlight different approaches to tech between Majority and Minority worlds, content moderation and policies focus on the experiences of wealthy nations. This means survivors in the Global South are at a greater disadvantage as often the support options available to them are in the form of therapeutic and law enforcement support and are limited.
- Law enforcement and criminal justice systems appear in many papers but there was a lack of in-depth acknowledgement considering the complex factors such as lack of awareness amongst legal systems and enforcement, systemic injustice, and cross-national crimes which means presenting this as the only way of getting justice for survivors misses out on all the reasons why survivors may not choose to do that. In many jurisdictions where trust in policing is low, survivors may prefer to get support and accountability from the technology companies themselves or other civic actors.
- Design discussions often focus on harm reduction and accountability but a more holistic approach must also include healing justice.
- Some papers mention the need for end-to-end encryption and PETs, while others don't. There seems to be a lack of consensus around this and it should be further explored.

Recommendations for Future Discussion

1. What are the entry points for influencing technology as a movement to support embedding principles for "safety-first design" in both mainstream technology and emergent technology?
2. How can we translate Feminist Design Frameworks into industry standards? Do we need a common guidance as an advocacy platform for influence?
3. What does "survivor-centred" mean in technology design and how can we ensure it is default in businesses?
4. How do we monitor and share best practices to support a process of continual improvement across GBV practitioners, organisations and technologists?
5. How can we create Global North/South equity in discussions of tech abuse?

Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004-3027

Wilson Center

The Wilson Center

www.wilsoncenter.org
wwics@wilsoncenter.org
facebook.com/woodrowwilsoncenter
@thewilsoncenter
202.691.4000

UNFPA

The United Nations Population Fund

www.unfpa.org
EndTFGBV@unfpa.org
@unfpa