ORBITS

A global field guide to advance intersectional, survivor-centred, and trauma-informed interventions to technology-facilitated gender-based violence

This guide was written by Hera Hussain (CEO, Chayn), Aiman Javed (Communications Lead, Chayn), Nishma Jethwa (Co-director, End Cyber Abuse), Esha Meher (Research Associate, End Cyber Abuse) and Naomi Alexander Naidoo (Head of Movement and Partnerships, Chayn). It was copyedited by Manal Khan. The guide was designed and illustrated by Carolina Moyano Izquierdo, with some illustrations by Beatriz Diaz.

With great gratitude to the Chayn team, trustees and volunteers for their contributions and reviews of this guide, in particular Nky Adeboye, Rachel Lebby, Antonella Napolitano, Sophia Raineri, Nissa Ramsay, and Dama Sathianathan. Thank you to Rebecca Rae-Evans and Beatriz Diaz who carried out interviews for this guide. Thank you to the wider End Cyber Abuse team for their contributions, reviews and research, in particular Akhila Kolisetty, Chitrangada Sharma, Habiba Akther, Sailaja Darisipudi and Naciza Masikini.

There are many more people who inspired and contributed to this guide - thank you all. Full acknowledgements can be found on page 115.

Thank you to the Robert Bosch Stiftung for making this work possible. A very special thank you to Anna Dorethea-Grass and Rana Zincir Celal for their guidance and support.

About Chayn

Chayn is a global non-profit that creates digital, multilingual resources to support the healing of survivors of gender-based violence. Our focus is on empowering women and other marginalised genders who have experienced domestic, sexual or tech-based abuse. Every decision we make – and every resource we create – has lived experience at its core.
So far, we've helped 400,000 survivors around the world. And – with a mission to make technology a tool for health, not harm – we reach more every day.

About End Cyber Abuse

End Cyber Abuse is a global collective of lawyers and human rights activists working to tackle technology-facilitated gender-based violence by raising awareness of rights, advocating for survivor-centred systems of justice, and advancing equitable design of technology to prevent gendered harms. We envision a world with equitable, safe digital spaces and technologies that are free from violence, oppression and harassment, that uphold the dignity and rights of people of marginalised genders.

Orbits

A global field guide to advance intersectional, survivor-centred, and trauma-informed interventions to technology-facilitated gender-based violence.

1 Introduction 1

1.1 About Orbits: addressing failures and gaps in technology, research, and policy 2

1.2 The Orbits journey: creating this guide 4
1.3 Orbits principles 5
1.4 How to use this guide 7

2 Understanding tech abuse and its impact 8

2.1 What is TGBV? 8
2.2 Taxonomy of tech abuse 12
2.3 The impact of tech abuse on survivors 18
2.4 Survivor Stories 19

3 How systems are failing survivors 25

3.1 How technology enables abuse 25
3.2 When research creates harm 34
3.3 The pitfalls of policymaking 38

4 Building better systems 50

4.1 Transforming technology: designing for healing 50
4.2 Rethinking research: enrichment not extraction 71
4.3 The potential of policy: justice and care 87

5 Further explorations 100

6 Conclusion 101

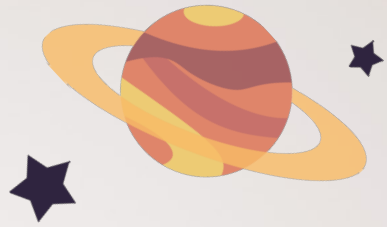
7 Glossary 102

8 Tools 103

9 How to build policy using the Orbits principles 104

10 Orbits library 112

11 Acknowledgements 115



Introduction

Modern technology has touched and transformed almost every aspect of our lives - the way we work, communicate, shop, eat, have fun, protest, and even access vital services and healthcare. It has transformed business, finance, civil society, media, and politics. It has brought opportunities, efficiencies, and innovations that were barely conceivable just a few decades ago. Many of the visions of sci-fi and fantasies of the future once previously imagined are now here.

However, when viewing how technology has transformed the world, it is far from a picture perfect. Technology has entrenched inequalities, polarised political and civic debate, and created novel and egregious safety and security risks. It has also created a myriad of new harms, such as the detrimental mental health impacts of social media, negative consequences of constant use of technological devices on our bodies, the environmental and climate impacts of technology production and use, and the use of new platforms to perpetuate abuse and violence. This guide will focus on one such harm: technology-facilitated gender-based violence (TGBV), or 'tech abuse'.

Gender-based violence (GBV) is not new. Around the world, one in every three women will experience gender-based violence in their lifetime. Transgender and gender non-conforming people face an extreme culture of violence. While GBV is an ongoing global crisis, advancements in technology have deepened, expanded, and complicated the issue. And as technology use, access, and functionality increases, so does this form of abuse.

1.1 About Orbits: addressing failures and gaps in technology, research, and policy

Orbits is a joint initiative of Chayn and End Cyber Abuse. Building on our joint expertise in tech abuse, and insights and feedback from our communities and the global ecosystem, we are collectively working to stop TGBV.

Chayn is a global non-profit that creates digital, multilingual resources to support the healing of GBV survivors. Since 2013, hundreds of hours of researching, creating, testing, learning, unlearning, and experimenting have gone into how Chayn's design supports survivors across different types of needs, languages, cultures, and political landscapes. End Cyber Abuse is a global collective of lawyers and human rights activists working to tackle technology-facilitated gender-based violence by raising awareness of rights, advocating for survivor-centred systems of justice, and advancing equitable design of technology to prevent gendered harms.

Tech abuse is an incredibly complex problem that transcends borders, sectors, and jurisdictions. Tackling it effectively will therefore require nuanced, impactful interventions from diverse stakeholder groups across multiple fields, such as media, education, and national and international law. This guide focuses on three areas that we believe are vital in the fight to end tech abuse: technology, research, and policy.

To address TGBV, first and foremost we must look at technology. As the tools through which tech abuse is carried out, the design and governance of tech products and services is instrumental to how abuse is perpetrated and how it can be stopped. Within this, we look at both technology design and 'little p' policies the internal policies, practices, and guidelines of tech companies that regulate their community.

Research is also crucial to properly understand the phenomenon of tech abuse, its different forms and manifestations around the world, and the experience of and impact on survivors. It is only through a well-researched and nuanced understanding of the problem that we can design interventions that will effectively address the problem. Equally, user research informs product development in technology - and we will pay particular focus to that type of research in this guide.

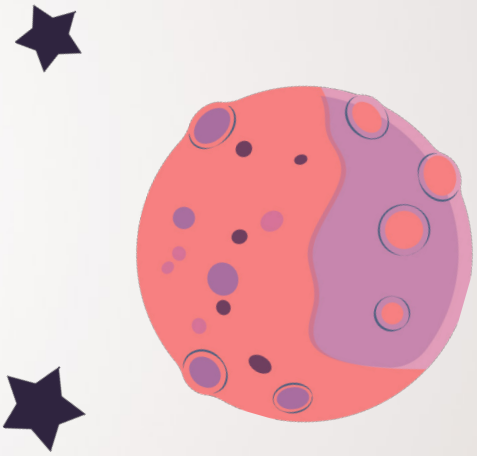
Lastly, the policy landscape governs the systems which enable tech abuse. Here, we mean 'big P' policies - criminal and civil law focusing on survivors, and regulations targeted towards the private sector. Effectively tackling tech abuse will require a transformation of both.

Based on Chayn and End Cyber Abuse's work and learnings on tech abuse to date, we identified three lenses that are noticeably missing from the prevailing responses to tech abuse but are imperative to tackling it effectively. Orbits therefore advocates for an approach which is intersectional, survivor-centred, and trauma-informed.

Intersectional: By intersectional, we mean the way systems of oppression overlap and intersect to produce particular experiences for different people around the globe. Taking an intersectional lens means acknowledging that oppression does not exist in silos. It means considering how different systems of oppression - including patriarchy, racism, socioeconomic inequality and more - shape the world we live in and our individual experiences within it.[1]

Survivor-centred: To be survivor-centred is to keep survivors and their diverse perspectives at the centre of everything we do. While every survivor is different, each survivor holds expertise in their own experience. This expertise is invaluable in tackling problems in a way that respects survivors' agency and knowledge. Taking a survivor-centred approach means building interventions with, and not just for, survivors.

Trauma-informed: A trauma-informed approach understands and acknowledges the nature and impact of trauma. Trauma is an emotional response to one or many events that pose a risk of harm or danger to the survivor or to others. Being trauma-informed means responding to and working with this complexity.[2] These three lenses shape this field to addressing TGBV.



[1] The term intersectionality was coined by feminist legal scholar, Kimberle Crenshaw, in 1991, when she addressed the law's failure to consider the particular discrimination that African American women experienced. The law at the time could only account for experiences of oppression along one axis, so legally, African American women could only experience discrimination for their race or their gender but not their intersecting identities.

[2] Trauma is not prescriptive. It evokes different reactions for different people, but can include feelings of fear, humiliation, rejection, abandonment, shame, and powerlessness. It can make us feel unsafe in our bodies, minds, and within our wider communities. The impact of trauma can affect a whole group of people and even extend beyond our lifetime through intergenerational trauma. But where there is trauma, there is room for healing. Every survivor's journey is different - while there is a tendency to oversimplify what it means to 'heal' to make it more convenient as a process, healing is messy, non-linear, and can take any length of time. There might not be a 'before', a 'normal' self without trauma, or an 'after' — which implies that suffering made someone stronger or better or simply different. Especially for survivors where there have been cycles of abuse or they have been abused since childhood (whether in their familiar or close relationships or by larger systems of power), there is often no before or after.

1.2 The Orbits journey: creating this guide.

Orbits is a project funded by Robert Bosch Stiftung's "Reducing Inequalities Through Intersectional Practice" fund. While we started this project in January 2021, both Chayn and End Cyber Abuse have been addressing tech abuse for many years. This guide builds on and develops our existing expertise and experience in this field.

In developing this field guide and accompanying resources, we worked through three key phases; documentation, enrichment, and reflection. First, we sought to document our organisational practices - working to address tech abuse by directly supporting survivors and through advocacy and policy work. We shared our journey and our learnings on the Orbits blog. We sought to reflect and understand our own ethos and approaches to intersectional, survivor-centred, and trauma-informed practice as organisations. This involved outlining our existing design principles and recommendations.

In the enrichment phase, we sought input and ideas from the wider ecosystem. We interviewed nine practitioners and activists around the world who are working to address tech abuse in their respective regions - quotes from these interviews can be found throughout this guide. We did in-depth interviews with four survivors of tech abuse who told us their stories, and also held participatory consultation workshops with participants from across the world, including researchers, activists, campaigners, UX designers, and survivors.

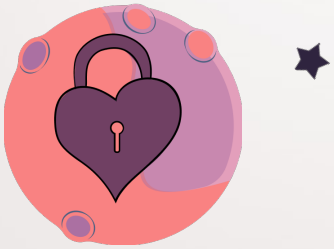
Meet our Orbits experts who we interviewed for this guide:

- ★ **Lulú Barrera, Mexico - Founder of Luchadoras**
- ★ **Chenai Chair, South Africa - Special Advisor for Africa Innovation at Mozilla Foundation**
- ★ **Nighat Dad, Pakistan - Founder of Digital Rights Foundation**
- ★ **Bishakha Datta, India - Executive Director at Point of View**
- ★ **Sarah Fathallah, USA - Independent social designer and researcher**
- ★ **Mary Anne Franks, USA - Professor of Law at Miami Law School**
- ★ **Shmyla Khan, Pakistan - Director of Policy at Digital Rights Foundation**
- ★ **Chanelle Murphy, USA - Trust & Safety Product Manager at Pex**
- ★ **Mariana Valente, Brazil - Director at Internet Lab**

We then spent time reflecting on this enrichment phase to adjust, synthesise, and finalise our documentation. In line with our commitment to co-create the guide with peers and partners, we shared a draft guide with our community for comment. This final guide reflects their feedback and knowledge. A list of all contributors who wanted to be named can be found at the end of the guide.

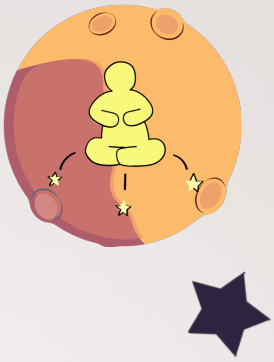
1.3 Orbits principles

Through the Orbits journey, we developed eight principles to guide our work to tackle tech abuse. These principles are the foundation of our approach to designing intersectional, survivor-centred, and trauma-informed interventions and can be applied across tech, research, or policy work. They form the bedrock and scaffolding for the rest of this guide and will be referenced throughout.



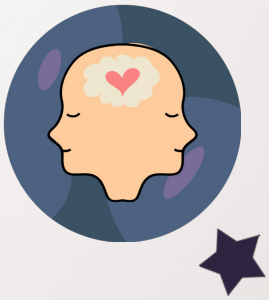
1. Safety

We must make brave and bold choices that prioritise the physical and emotional safety of people, especially if they have been denied this safety at many points in their lives. Whether it is the interface of our platform or the service blueprint, safety by design should be the default.



2. Agency

Abuse, inequalities and oppression strip away agency by removing the survivor's power and control over their narrative. We must not use the same tactics of oppression and abuse in our design. Instead, by honouring the survivor's wishes in how their story is told and used, we can create an affirming experience. This requires seeking informed consent at every step and providing information, community, and material support to survivors. Users should be critical to their own path to recovery, and be involved in how the interventions are designed.



3. Equity

The world as it currently exists is not just. Systems are set up to favour dominant groups, without doing justice to the differing needs of people. As such, all of our interventions need to be designed with inclusion and accessibility in mind. Survivors are not a homogenous group; everyone will not benefit from the same types of support. We must consider how position, identity, vulnerabilities, experiences,

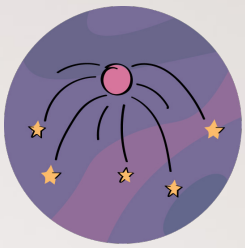
knowledge, and skills shape trauma and recovery, and focus on creating solutions that leave no one behind.

4. Privacy

Privacy is a fundamental right. Due to stigma, victim blaming, and shame associated with gender-based violence, the need for privacy is greater. A survivor's personal information, such as data, images, videos, or statements, and their trauma story, must be kept secure and undisclosed, unless the survivor decides otherwise. At the same time, we should ensure that survivors are able to access the help and information they need by removing any unnecessary obstacles that may come their way.

5. Accountability

We must build accountability into the harm, and the interventions that address it. This includes being open and transparent about what is being done, how, and why; we must create and nourish constructive feedback loops that trigger change. It also means openly communicating about what is working and what isn't. To build trust, this communication should be clear and consistent.



6. Plurality

There is no single-issue human, and to do justice to the complexity of human experiences, we need to suspend assumptions about what a person might want or need and account for selection and confirmation bias. Harms manifest in different and disproportionate ways for people living at the intersection of multiple oppressions, these lived realities must be recognised and we should never assume a 'one-size-fits-all' approach

7. Power redistribution

Too often, the power to make decisions is concentrated in the hands of a few. Instead, power must be distributed more widely among communities and individuals who are most impacted by TGBV. Interventions should be co-designed and co-created with survivors.

8. Hope

Abuse can leave us feeling hopeless. We should not use harsh words and upsetting pictures which can possibly remind survivors of their own struggles, experiences, or difficulties. Interventions should be designed to be an oasis for users, by being empathetic, warm, and soothing, motivating people to seek and embrace the help on offer. It should validate their experience as we seek out collaborative solutions and offer hope for the future. We must not use sensationalism or shock value for the sake of a wider audience. Instead, our focus should be on survivors and their healing.

1.4 How to use this guide.

The Orbits field guide is a resource for anyone working to end tech abuse. It is particularly relevant for technology companies, designers, non-profits, civil society organisations, activists, researchers, and policymakers.

It is intended to be a practical resource to support designing interventions in technology, research, and policy-making. It does not include a detailed theoretical analysis of tech abuse, its roots, causes, and effects. There is a rich body of scholarship that is dedicated to addressing tech abuse in this way, and we point to some of it throughout the guide and in the guide library. We're grateful for the work of academics and activists who have led this conversation and who inform our work.

Tech abuse is a complex, multi-faceted issue and we know that one guide cannot address every instance and nuance of tech abuse or intervention to it. We also know that it is fast-evolving so anything that is written can quickly become dated. But we hope that this resource will help you deepen your understanding of tech abuse and the need for an intersectional, survivor-centred, and trauma-informed approach to tackle it. We hope it provides you with tools that you can apply and adapt, based on your context and work.

Orbits includes:

- ★ **Narrative analysis:** The guide starts by exploring the issue of TGBV, what it is and how it impacts survivors. It then looks at how current systems in technology, research and policy are failing survivors. Finally, it suggests how we can build better systems across these three areas and suggests some areas for further exploration.
- ★ **Survivor stories:** To illustrate the full nature of TGBV, we profile the true stories of four different survivors from around the world.
- ★ **Case studies:** Case studies are placed throughout the guide to demonstrate what the Orbits principles look like in practice.
- ★ **Quotes:** Standout quotes from the interviews we carried out with experts are interspersed around the guide.

★ **Sign-posts:** Throughout Orbits, we sign-post to inspiring initiatives and materials on TGBV from around the world.

★ **Library:** A collection of great resources and research, about TGBV.

Navigation station

Interested in technology?	Head to chapters 3.1 and 4.1, pages 25 and 50.
Want to read about research?	Go to chapters 3.2 and 4.2, pages 34 and 71.
Would you like to learn about policy?	Turn to chapters 3.3 and 4.3, pages 38 and 87.
Ready for lift off and want to work the Orbits tools?	Head straight to the toolbox on page 103.

2 Understanding tech abuse and its impact

Technology does not exist in a vacuum. It is shaped by the society in which it is produced. Where there are systems of oppression and harm (such as racism, sexism, casteism, disablism, homophobia and transphobia), they will invariably be replicated in the tech space as well. This is the case with TGBV.

2.1 What is TGBV?

The United Nations defines GBV as "harmful acts directed towards an individual or a group of individuals based on their gender."

This includes sexual, physical and emotional assault, abuse, and violence. Tech-facilitated gender-based violence, then, is any such violence that is carried out through or enabled by technology. It is an extension of other forms of GBV and does not exist in a silo. Often, TGBV occurs in interaction with other forms of GBV, which include offline violence and harm.

"[There is a] spectrum of violence in terms of trying to define online gender-based violence: the experience of emotional and physical harm that manifests in the online space and can be taken through to the offline space and vice versa, from offline to online."

Chenai Chair, Mozilla Foundation

The increase in accessibility and rapid development of tech have given rise to new and scary ways in which GBV can be inflicted. As a result, incidences of tech abuse have soared. Research carried out by the Economist Intelligence Unit in 2021 found that globally, 38% of women have experienced online violence personally.

A further 65% have witnessed violence targeting other women, meaning 85% of women have experienced tech abuse in some way. The figures are higher among younger women: 45% of women who are millennials or belong to generation Z report personal experiences of online abuse. Plan International's Free To Be Online? 2020 report surveyed 14,000 young women and girls across 31 countries and found even more alarming statistics: 58% experienced online harassment, 50% experienced more online harassment than street harassment, and the majority of girls who get harassed online for the first time are between the ages of 14 and 16.

> *"It's not a new manifestation of violence. Rather, it's the same old system, using the new technologies to perpetuate itself and even, worsening some points because of aspects of the online space... that it could get more viral, it could reach more people, it could last much longer on the webspace."*
>
> Lulú V. Barrera

The problem became even more acute during the COVID-19 pandemic, as lockdowns around the world forced us to shift almost every aspect of our lives online. Globally, there was such a sharp rise in domestic violence that it has been referred to as 'the shadow pandemic.' It is estimated that incidents of domestic violence increased by around 20% around the world: in France, cases increased by 30%; in Argentina, calls to emergency services rose by 25%; in Cyprus, helpline calls went up 30%, and Singaporean helplines received 33% more traffic.

This abuse spread into digital spaces as well. In the UK, Refuge experienced a 97% increase in complex tech abuse cases from April 2020 until May 2021 in comparison to the first three months of 2020. In the Philippines, Foundation for Media Alternatives (FMA) mapped 130 reports of tech abuse in the media, which is a 165% increase in comparison to 2019 and the highest number of cases since FMA started mapping this data in 2015. Online stalking also increased. Suzy Lamplugh Trust, a UK charity working to create safety from violence and stalking, found that of those who experienced stalking before the lockdown, 49% saw an increase in online stalking during the pandemic, and 100% of their cases now involve some cyber element. Globally, antivirus company AVAST reported a 51% increase in spyware and stalkerware detection within the first month of lockdowns being implemented in March 2020. Similarly, Malware bytes reported a 780% increase in the detection of monitoring apps and 1677% increase in the detection of spyware from January 2020 to December 2020. Research by Kaspersky found that 30% of people see nothing wrong with secretly monitoring their partner.

People with other marginalised identities or in marginalised professions are even more likely to experience tech abuse. For example, Glitch and End Violence Against Women Coalition surveyed nearly 500 women and non-binary people in the UK to learn about their experiences of online abuse during the pandemic for their report The Ripple Effect. 46% of respondents reported online abuse since the beginning of COVID-19 - for Black and minority respondents, the number was 50%. Several studies find that LGBTQ+

individuals are more likely to experience image-based sexual abuse (IBSA) than heterosexual individuals. Sex workers face widespread tech abuse including doxxing and image-based abuse, where their content is shared without their consent. Research in Australia shows that migrant women are particularly vulnerable to abuse in relationships via control of devices and digital media.

While these figures are already alarming, it is important to note that tech abuse, like other forms of GBV, is exceptionally underreported. 1 in 4 women report online abuse to the platforms where it takes place, and 14% report to offline agencies. There are many reasons for under reporting, including shame, stigma, and the unavailability and inaccessibility of support and reporting mechanisms. For tech abuse in particular, lack of awareness means that many survivors do not know that they are experiencing abuse, leading to further underreporting. Moreover, the failure of relevant authorities and institutions to take action leads to survivors feeling that reporting is useless.

This means that the numbers available to us present only a fraction of the actual picture. There should be no denial of the severity of the issue.

A note on terminology

In this guide, we use the terms technology-facilitated gender-based violence (TGBV) and tech abuse interchangeably. When we refer to tech abuse, we do not mean other forms of non-gender-based abuse, although in some cases the analysis may apply beyond gender-based violence.

Other common terms which are used to refer to TGBV, or part of it, include: technology-facilitated abuse; technology-enabled abuse; technology-mediated abuse; technology-facilitated coerceive control (TFCC), online violence against women and girls (OVAWG); online gender-based violence (OGBV); online violence; online sexual exploitation and abuse (OSEA); cyber abuse; cyber violence; electronic gender-based violence (EGBV); and electronic violence against women (EVAW).

Tech abuse takes many different forms. Some are very familiar - preexisting forms of abuse, replicated in a digital space - while others are more novel - perpetrators exploiting tech functionalities to harm survivors in new ways. Some forms of tech abuse are already prevalent all around the world, whereas some are specific to particular regions. Almost all forms of tech abuse are shaped by the cultural, social, and political context in which they take place, so the manifestation varies in different parts of the world and for different communities. While there are distinct forms of tech abuse, none of them exist in isolation - different tactics are often used in combination and can form part of larger patterns of abuse or coercion that straddle both online and offline spheres. For example, when surveying survivors of online domestic abuse, UK charity Women's Aid found that 85% reported that the online abuse perpetrated by a partner or ex-partner was part of a larger pattern of abuse which they also experienced offline. While online GBV often refers specifically to GBV facilitated through the internet, technology-facilitated gender-based violence encompasses

GBV carried out using any technology, including abuse perpetrated by older forms of technology such as telecommunications. As tech is constantly evolving, new forms of tech abuse continuously emerge.

"One of the nuances we see is GBV is often thought to occur predominantly on social media, and there is no doubt that social media is a site of TGBV, but in low income communities it's really through the mobile phone, and it's often through text messaging or through phone calls, just like a regular mobile phone call, that GBV takes place." -

Bishakha Datta, Point of View

2.2 Taxonomy of tech abuse

This section includes a non-exhaustive list of common forms of tech abuse that we refer to throughout this field guide.

Creep shots (upskirting/ downblousing)

Creepshots refer to the use of mobile phones and cameras to take 'up the skirt' or 'down the blouse' images of someone without their consent. Such images are generally taken of unwary users of public transport, restrooms, and elevators and are sometimes also circulated or published online. In the UK, police receive upskirting reports from at least one survivor every day, including many children.

Cyberflashing

Cyberflashing is the sending of unsolicited sexually explicit images or videos, without the receiver's consent. It is also commonly known as 'sending unsolicited d*ck pics'.

This can be experienced as a one off event or part of ongoing abuse and harassment. It can also include one or multiple images and/or videos. While cyberflashing can be perpetrated by someone known to the victim via social media accounts, dating apps and messaging platforms, it can also be done in public and by strangers using Bluetooth and AirDrop technologies. Many international studies found that around 50% of young women aged 18-25 have received penis images without consent, with prevalence increasing for girls under 18. A 2020 University College London survey of 150 young people aged 12-18 in the UK revealed that 76% of girls under 18 have been sent unsolicited sexual images on social media.

Cyber harassment/online harassment

Cyber harassment is the repeated harassment or threatening of an individual(s) in digital spaces. This often includes persistent unwanted communication and hateful comments. It might also include making threats of further offline abuse, such as physical or sexual violence.

While anyone can experience cyber harassment, those with multiple

marginalised identities are targeted disproportionately, and the problem is particularly acute for women in the public sphere, such as politicians, journalists, and activists. For example, in the USA, female legislators are 3.5 times more likely than male legislators to receive threats of bodily harm on Twitter, and politicians who are women of colour are twice as likely to receive tweets about their gender or body as their white women counterparts. Pollicy carried out a study into online violence during the 2021 Ugandan general elections, and found that women candidates were more likely to experience trolling (50% vs. 41%), sexual violence (18% vs. 8%), and body shaming (14% vs. 11%) in comparison to their male counterparts.

Research by Amnesty International on India's 2019 election found that one in every seven tweets sent to women candidates were abusive or problematic, and Muslim women received 55% more abuse than others. In the UK, Amnesty International carried out research into the online harassment of women members of parliament (MPs) active on Twitter in the run up to the 2017 general elections and found that 20 racialised female MPs received 41% of the abusive tweets, despite there being almost eight times as many white women in the research. The UK's first Black female MP Diane Abbott received nearly a third (32%) of the overall abuse.

Cyber stalking

Cyber stalking involves the monitoring of an individual's location and activities through geo-location trackers or monitoring their use of the internet. This might involve closely following their social media activity to find out where they are - for example if they post a photo in a recognisable place, geo-tag an upload with a location, or 'check-in' to a venue. It can also involve employing stalkerware to track someone's movements and actions. Intimate partners, as well as strangers, resort to cyber stalking, and it is often part of a larger pattern of controlling and coercive behaviour, including offline stalking. Cyber stalking can also involve using wearables and tracking devices, such as AirTags.

Digital morphing/Deepfakes

Digital morphing is the use of technology like Photoshop or AI to create a photograph or video, in which a person's face is morphed or superimposed on the image of another person's body. Perpetrators use, or pay another individual to use, such

morphing technology to create fake nudes, explicit images, or videos. These are often used to perpetrate further forms of image-based abuse as outlined below. A 2018 analysis of 7,964 videos, by Amsterdam-based cybersecurity company Sensity (formerly Deeptrace), found that 90% of deepfake content online involves non-consensual deepfake pornography, where women's faces are superimposed onto naked or sexual images.

Out of the top 10 pornographic websites that host deepfakes, nine websites are monetised entirely by them. An investigation into a version of the app DeepNude on the messaging app Telegram revealed that over 680,000 women had their images stolen from their social media accounts or private conversations, which were then manipulated and sexualised. Terrifyingly, the number of deepfakes on the internet is thought to double every six months.

Doxxing

Doxxing is when perpetrators purposefully leak previously private and personal information online. By publishing details like name, contact number, email address, and home and office address publicly, victims are exposed to unwanted attention and possible harassment, threatening their safety and mental health. A 2021 study by SafeHome found that 21% of Americans, over 43 million people, had experienced doxxing.

Gendered disinformation and gender trolling

Gender trolling is when gender-based insults or hate speech are shared online. Similarly, gendered disinformation involves the spreading of false or misleading gender-based narratives, often with some degree of coordination. Common false narratives include those manipulating gender stereotypes about women, lying about gender equality, and fabricating information and statistics about contentious issues related to gender. In all cases, the sharing of such speech is often coordinated by groups, meaning survivors experience a barrage of such messages. This form of abuse is often intended to deter women from participating in public life.

Image-based abuse

Image-based abuse includes all forms of non-consensual taking, creating, altering, or sharing of (including threats to share) intimate images or videos. While this is generally understood as

referring to sexual or nude images, we define 'intimate images' as any image which shows someone as they would not normally be seen in public. For example, for someone who usually wears a headscarf or other form of religious garb, a photograph of them without it would constitute an intimate image. Image-based abuse is often referred to as 'revenge porn', but this term is generally rejected as such material should not be viewed as porn nor revenge and the term obscures the complexity of the issue.

There are often multiple, overlapping motivations for image-based abuse, including harassment, humiliation, and public shaming, status-building among groups of men, sexual gratification, and sometimes financial gain. The perpetrator may leverage image-based abuse to get a survivor to stay in the abusive relationship, for sexual favours, for money, or to scare or silence them from disclosing abuse. Threatening to share intimate images is image-based abuse, regardless of whether the images are actually shared or not.

Sex workers are particularly at risk of image-based abuse, as their content is often distributed without their consent. A study by LegalJobs in 2021 found that pornography is one of the most pirated materials on the web, with an estimated 35.8% of pornographic material being pirated online. Similarly, a recent investigation discovered "an entire supply chain of people stealing sex workers labour using scraping programs without permission, in some cases by the hundreds of terabytes, and distributing it on other adult sites or selling scraping services through Discord."

Refuge, a UK based organisation that works with victims of domestic violence, conducted a survey of 2,060 people in 2020, and found that 1 in 14 women had been threatened with image-based abuse. For young women aged 18-34, this number rises to 1 in 7.

Impersonation

Impersonation is when a perpetrator uses technology to pretend to be someone else. Typically, a perpetrator creates fake social media accounts using the name and image of the person they are impersonating. They may use these accounts to share content or send messages that are harmful to the person in question, such as sending obscene or offensive messages to their personal or professional contacts.

Outing gender identity or sexuality

The outing of a person's gender identity or sexuality may be done on online platforms, either publicly or to their family and friends without that person's consent. This kind of abuse targets LGBTQ+ people who may not have disclosed their gender or sexual identity to everyone or certain people.

The caller may pretend that the call is a misdial or will hang up every time the call is answered. This form of harassment is particularly common in lower-income, rural communities, for example in India.

Repeated wrong dials

Repeated wrong dials refers to the instance where someone is regularly 'miscalled' by another individual, often from an unknown number.

For example, many young men are being groomed into misogynistic attitudes online, which in turn produces perpetrators of TGBV (and other forms of GBV).There are other forms of online abuse and harm that are beyond the scope of this guide, including identity theft, use of opaque algorithms, online scams, and online child exploitation. For an overview of different categories of online harm, see the Online Harassment Field Manual.

Smart-home abuse/domestic digital abuse

Smart-home abuse is when a perpetrator manipulates technology or Internet of Things (IoT) devices that control someone's home environment, for example light, sound, temperature, or locks. This kind of abuse is usually seen in the context of domestic abuse as part of coercive control. An abuser might make the home excessively hot or cold, might switch lights on or off, or play music or noises to impact their partner's physical and mental wellbeing. Devices used for smart-home abuse include ring doorbells, Amazon Alexa and Echo, Google Home Hub, CCTV cameras, and more. Often this abuse is carried out via smartphone apps, even if the abuser is far from home. Smart-home abuse can also involve intrusive tracking through digital devices, such as watching someone's movements through sensors or security cameras, or eavesdropping through microphone-enabled smart devices.

Zoom bombing and Zoom flashing

Zoom bombing takes place when individuals disrupt online video calls without authorisation and inundate participants with unsolicited and disturbing content, such as graphic sexual images, videos or/and derogatory words. Zoom flashing is when someone exposes their genitals live online after infiltrating an online meeting. These activities have increased during the pandemic, when most work and education shifted to online platforms. Named Zoom bombing because of the popular video-conference tool Zoom, it can happen on any video-calling software including Skype, Microsoft Teams, and Google Meet.

While Orbits focuses on TGBV, there are other forms of online or technology-facilitated harm which impact women and people of marginalised genders.

2.3 The impact of tech abuse on survivors

> *"Some victims had to move from the town they live in. Some people, like the founder of our organisation, have had to change their names. Some have died by suicide."*
>
> Mary Anne Franks, Miami School of Law

Like all forms of GBV, tech abuse can be devastating for those who experience it. While the impact on each survivor is different - it may be influenced by a range of factors including the nature of the abuse, where the survivor is based, their personal life circumstances, and different aspects of their identity - there are several common themes for the way tech abuse affects survivors.

Physical safety

Online violence often endangers and impacts a survivor's offline physical safety. In some cases, this form of abuse can be carried out by perpetrators who first identify the survivor through some form of tech abuse and then continue to stalk, harass or threaten them. In some cases, survivors' physical safety may be threatened by family members or other close contacts, who carry out violence as a disciplining or punishing act.

Mental health

The impact on survivors' mental health can be deep and serious. Instances of post-traumatic stress disorder (PTSD), paranoia, anxiety, and depression are recorded frequently. Many survivors report severe trust issues and self-image problems as a result of tech abuse. For many, the impact is long-term as they do not regain the confidence or sense of safety they had before the abuse. They may restrict their use of technology, or withdraw from online spaces completely. The helplessness that ensues when one is unable to control their information on the internet gives rise to prolonged trauma that often manifests in unpredictable ways. Some may have suicidal thoughts or move towards a more reclusive life. The lack of help or support pushes many to find their own coping mechanisms, which can lead to further issues like drug abuse, alcoholism or self harm. 35% of survivors report mental health issues as a result of experiencing online violence, and 43% feel unsafe.

Relationships

Due to stigma and prejudice against them, survivors often experience a severe negative impact on their relationships. Given that many forms of tech abuse involve a public element (for example, sharing intimate images publicly or with a survivor's friends/family/acquaintances), this a particularly pertinent concern. Even if the abuse does not involve a public component, survivors often face this impact if and when they decide to disclose their trauma to those around them. Some survivors are completely ostracised by family members and/or social and professional circles.

Often, they experience victim blaming, where they are blamed for the violence inflicted upon them. 23% of survivors said that their experience of tech abuse had caused harm to a personal relationship. The negative impact on relationships can create feelings of loneliness and isolation, which in turn often contributes to further mental health consequences.

Reputation

Often, perpetrators of tech abuse use survivors' reputation as leverage to inflict harm. A survivor may suppress the instance of abuse or continue to maintain a relationship with the perpetrator in an attempt to preserve their reputation. But when tech abuse is disclosed, whether by the perpetrator or the survivor, the social backlash can be extensive. Survivors have lost jobs, been expelled from school, college, or university, had to change their identities, and even relocated to different cities. Often survivors feel they have to completely change their lives to create a new image and reputation and leave behind the so-called 'tarnished' one.

Economic

There are often serious economic impacts for survivors of tech abuse. The experience itself can create multiple costs (legal fees, therapy costs, replacing compromised devices), whilst the reputational impact can create further costs (the cost of relocation or losing your job) and impair a survivor's ability to generate income by impacting their employment prospects.

Self-censorship

Tech abuse can inhibit a survivor's freedom of expression as they may self-censor, or remove themselves from the online sphere completely due to shame and fear of further abuse 58% of those surveyed in a global survey titled 'Free to be online?', conducted by Plan International with 14,000 women respondents from 22 countries, have experienced online harassment on platforms such as Facebook, Instagram, Twitter, WhatsApp, and TikTok. 19% of these girls reported leaving or reducing usage of specific social media platforms after being harassed, while 12% stated that they changed their behaviour on digital spaces to avoid harassment.

Tech abuse can even have a silencing effect on those who have not experienced it directly. Knowing about the existence and prevalence of tech abuse can sometimes be enough to discourage people from having a presence on social media and/or taking up public positions. This in turn entrenches gender inequality, by providing additional barriers to women taking up positions of power and/or expressing themselves. Nearly 9 in 10 women restrict their online activity, and 1 in 3 think twice before posting any content online.

2.4 Survivor stories

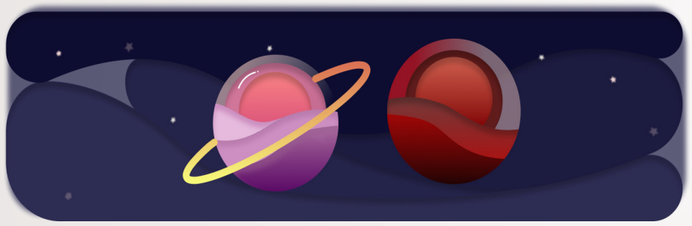
To fully understand the nature and impact of tech abuse, we must look to the stories of survivors. The following are true stories, based on interviews with survivors, but their names and some other details have been changed for anonymity. These stories demonstrate the many different ways tech abuse can manifest, how it is interwoven with offline activities and other forms of abuse, how tech abuse can occur as one-off incidents as well as part of long-term patterns of abuse, and how difficult it can be to find support and/or seek justice.

“It’s a kind of abuse that no-one ever faced I think,” she says. “Nobody knows what I’m talking about. Nobody understands what I’m talking about. It’s so complicated that I’m searching for answers.”

Huma’s story

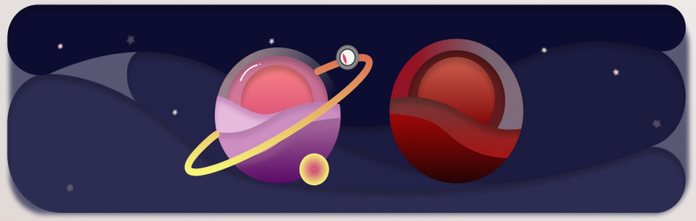
In the ten years Huma was married, she faced multiple forms of violence, including non-consensual recording - a form of tech abuse.

When 20-year-old Huma got married in her native country, Pakistan, the controlling behaviour began immediately. She wasn’t allowed to pursue her education, or visit her parents and relatives, especially male cousins. A year into the marriage, Huma had her first son. Her husband and mother-in-law continuously reprimanded her for not being a good mother, and falsely accused her of neglecting the child. Meanwhile, her husband wouldn’t sleep in the same room to avoid the noise of their newborn son.



A year later, the couple moved to Saudi Arabia where the abuse escalated to frequent physical violence. On one occasion, her husband split open her eyebrow in front of her mother-in-law, who pretended nothing happened. Unfortunately, this was just the tip of the iceberg.

“ I experienced severe emotional, mental, financial, physical abuse”

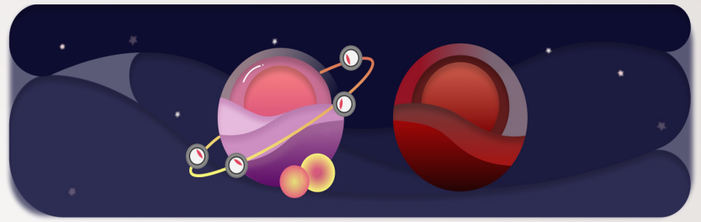


Eventually, the husband began to abuse her using technology, which became one of his central methods of control. Huma first experienced tech abuse when the couple and their son took a trip to Pakistan, to visit Huma’s mother-in-law. During that trip, Huma’s husband accused her of having sex with another man in her room. She denied this, reminding him that they were in his mother’s house, and the only other man there was his brother. At this point, he revealed that he’d downloaded an app on their son’s iPad to detect sounds nearby, and insisted he had heard her having sex with another man. “I was just crying miserably: no I didn’t do anything, I didn’t do anything,” she shares. Shattered, she went to his mother who spoke to him and calmed him down. Nevertheless, it became a point of contention that he repeatedly brought up in the years that followed.

Four years into the marriage, a new form of tech abuse started developing. During arguments, Huma’s husband would record her and make videos with his phone. This would aggravate her further, and she’d try to stop him. Later, he would claim that he only wanted to stop her from fighting him, and that he had deleted the videos. “I trusted him throughout this marriage on everything he said,” she says.

The next year, Huma and her husband moved to the United States. There, the frequency of these recordings increased: “That is where it started to happen too often, too much. Every single fight he would do this.” He would start recording her whenever she tried to discipline their son. One day, she found a hidden camera installed in their kitchen. The husband said he was monitoring the house for security purposes, but when she challenged him, he admitted that it was to record her because he claimed that she was abusing their son. This became a common reason used to justify his actions. At one point, Huma says that the manipulation was so overwhelming that she began to believe that she was indeed abusing their child.

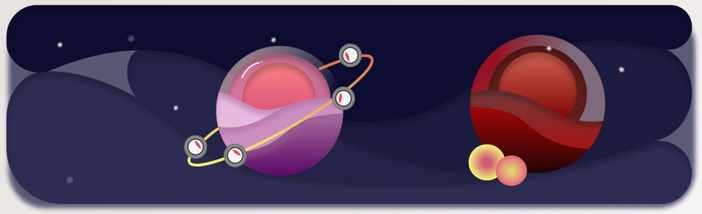
A few years later, the couple had another son. Again, the husband refused to sleep in the same room as their baby, so Huma and her newborn moved to a different room. Her husband set up a humidifier for her and would ensure it was turned on every night. This made Huma suspicious, so she searched the model online and discovered that it was a spycam. She dismantled it, and found another camera. Her husband initially acted surprised and threw the humidifier away, but later admitted that he had been recording her, using the same justification as before.



Additionally, he told Huma that she was bipolar and would joke about uploading videos of her on YouTube. Following this incident, her husband continued to record her with his phone. Though the couple spoke Urdu at home, he’d narrate the videos in English, saying she was abusing the baby who was asking for milk. Soon, Huma found another camera in the kitchen. This time, he said that he had placed it there because he feared that she could be poisoning their food. Meanwhile, he consistently threatened and manipulated her:

“Please be very careful. I have a library full of your videos. You will lose these children. These children will go to a foster home. You are an abusive mother. I’ve got you on camera where you are abusing the children. They are not going to spare you. You are going to jail. You’re not getting these kids. If you try getting out, just remember one thing: you are not getting the children, because I am going to show these videos to everyone.”

The marriage hit a turning point when Huma’s husband called the police after an argument with her, claiming she had hit him. While no arrest was made, the Child Protection Services (CPS) were informed and they opened an investigation. Soon after, the husband called the police again, alleging that she had harmed their youngest son. Before the police arrived, her husband fled, taking their older son with him. Over the next few weeks, she tried to get her son back but to no avail. At this point, she filed for divorce.

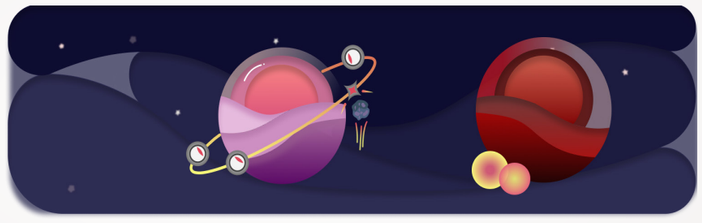


For her first hearing, she was sent the videos her husband was presenting as evidence. There were ten videos from cameras she had never found. In two videos, Huma was aggressive towards her sons. “I just sat there and I cried and I cried,” she says. “I was watching myself in these videos, and I knew that in court these videos were going to be on full-blown TV, and what am I going to do? Because I thought I’m never going to get my son back.”

However, after completing a two-month investigation, CPS ruled out any abuse. When the videos were played in the courtroom, Huma realised that no one blamed her. Her husband demanded that she should have a psychological examination, but the judge ordered for both to be examined. Her husband had also presented 23 videos as evidence but the examining psychologist asked for the videos to be translated for more context, validating Huma’s experiences. An amicus attorney also met the children, the families and saw the houses. A 40-page report was produced, which was completely in favour of Huma. “The amicus attorney said, ‘How dare you record your wife in front of your children? How dare you do that?,’” she says. Following this, the older son was returned to her.

Though this was a win for the survivor, the situation is far from resolved. Post-divorce, Huma now has shared custody of her children, so she has to keep interacting with her ex-husband. He continues to make threats about taking the children away and records everything to prove that he is a good father. Through a counsellor, the survivor has learnt not to respond to these texts but she worries about the wellbeing of her children. The husband’s house has four cameras installed, and this surveillance has been normalised for the older son.

Moreover, her ex-husband continues to record her when they meet to exchange the children. Huma is careful not to retaliate as she knows that he may use this against her. To address this behaviour, she once called the police to complain but they say they can’t help her unless her life is under threat. A lawyer from a non-profit has informed the survivor that her lawyer should have included a condition in their divorce agreement that stopped her husband from recording her. However, this did not happen, and it seems that all previous videos were also not seized from him.



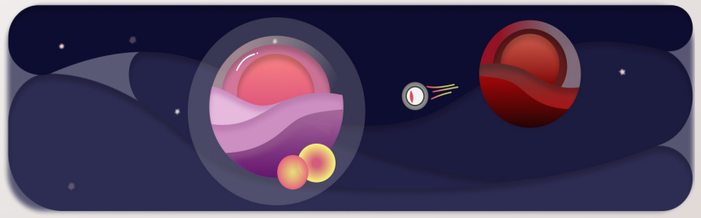
To add insult to injury, she later realised that her husband had also been cheating on her. Naturally, Huma is worried about all those videos her husband may have recorded during their time together, especially in intimate situations, since there is no clarity on how many cameras he had over the years, or when and where he had been using them. “All my life, the camera might be there recording it. Now I’m divorced, what is he doing with those videos?” she wonders.

Unfortunately, Huma isn’t free from physical violence either. In one instance, the ex-husband physically grabbed her at a doctor’s office. She filed a complaint about this assault but the case was dismissed. When Huma approached the prosecutor for an explanation, he implied that she was lying and acting in retaliation. This has severely damaged her trust in the legal system.

“When a person of authority says something like that, it really makes a big difference,” Huma says. “His words still ring in my ears when I think about it.”

Though Huma has now found a government website where she can register a complaint about the harassment, she is hesitant because of the lack of trust in authorities and the difficulties one encounters when trying to report such incidents.

“A lot of things would start again.” she says. “All of that would start again. I’m just scared and tired. I don’t want to go through it. I don’t know what the outcome will be, actually.”



“Even though I was not physically assaulted, this man assaulted my reputation sexually,” she says. “He was enabled by technology because he put it in a group.”

JayneRose’s story

A lawyer in Kenya, JayneRose was subjected to tech-enabled abuse facilitated by WhatsApp groups when she took a ride from a colleague one day.

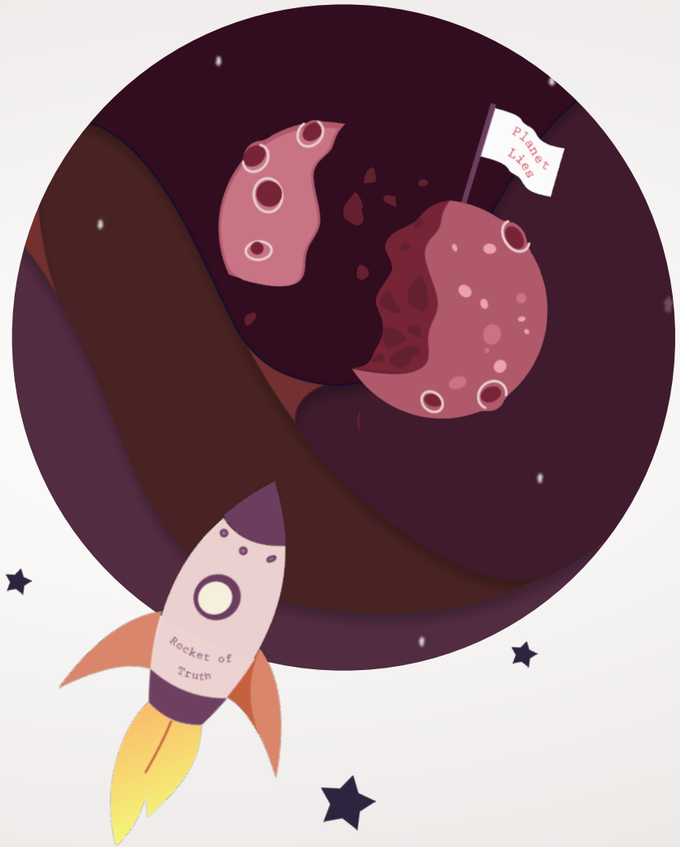
In May 2015, JayneRose took a bus to attend a law development seminar, in a town 100 kilometres from her hometown. A colleague offered her a ride back. On the way, he paused at his stepmother’s grocery store, where both greeted the stepmother, and then continued on their journey. JayneRose reached home safely.

Two years later, a male friend reached out to the survivor, to share the rumours that were circulating about her in legal circles. In a WhatsApp group, her colleague had disseminated a story about the day she took the ride from him. According to him, she’d had sex with him in a hotel after they met his stepmother, after which they’d also had sex outdoors, “in a bush”.

“He never left that bit out that we went to see the stepmother. So when people are asking me, have you ever been with this man, and have you ever seen his stepmother? I said yes, I know the stepmother.” Unknowingly, she’d been confirming the rumor. By mixing fact with fiction, the colleague had gained validity for this fake sexual encounter.

Later, JayneRose realised that this story had primarily been shared in all-male WhatsApp groups where men narrate such stories as a source of amusement. She says of the groups: “I think they had a list, that is what I concluded, for sharing wishful thinking or something.” The reference to the ‘bush’ was meant to inject humour into the tale. The friend who’d alerted her had himself felt guilty for being in such a group and for not standing up for her.

“Their work is to discuss their sexual encounters, real and imagined, with women. If, say you have turned down someone’s invitation or a date or a relationship, they actually go there and create their own stories.”



She identifies the usage of WhatsApp groups for abuse as a widespread problem in the region and advises everyone to first understand the nature and objective of such groups before engaging with them.

“If the aim of the group is not social progress, if it’s to defame people’s character, to abuse men or women or children, just get out of that group.”

Since two years had passed when she found out, she couldn’t file a case for libel or slander due to a statute of limitations. Moreover, she felt unsure of the support, if any, that she would receive from the other men in the group who had witnessed the abuse. However, she did confront him. “I said to him that you are very, very lucky that I cannot sue you because time has passed, but do not talk to me again and do not abuse me again,” she says. “Because if this happens again and I hear another bit of this story, it’s going to be very, very bad for you.”

Despite the confrontation, it’s an experience that continues to impact her. “For me it’s very important because the work I do, your reputation is everything,” she says. “Your character, how people view you, is everything. I always wonder, did someone fail to give me a job or look down on me because of a lie they heard about me?”

Today, JayneRose continues to be a successful lawyer, who shares her experience with young women in the legal circles as a cautionary tale. She is vocal about what happened to her, and urges women to support and defend each other, and avoid situations where they are alone with male colleagues. On some level, the incident is inhibiting JayneRose as she avoids professional gatherings. Moreover, it’s also affecting other women lawyers who hear about it.

“I always tell people: if you ever hear a story about a woman and it’s coming from a man, then you better not believe it.”

“There really wasn’t anything that I did about that, besides continue to have quite a low presence online. It again dug in that experience of just not feeling safe and the general feeling of unsafety and almost like you can’t turn anywhere. That is a really different feeling that I’ve had with the things that have happened online.”

Emily’s story

Three incidents of tech abuse have created a chilling effect on one survivor’s usage of the internet. Emily was sexually assaulted when she was 18 and has been cautious about her physical safety ever since. Her first experience of tech-enabled abuse was a few years after the assault, when she gave her number to someone she met in a gay bar, thinking their interaction had been friendly. The next morning, she woke up to a series of increasingly aggressive messages from them.

Disconcerted from this interaction, Emily clarified that she didn’t want to talk further and blocked the number, but for the next month, the messages kept pouring in via other platforms. As her number was linked to a social media profile which contained more information, it had been possible to track her down. “It was very much like constant harassment,” she says. “I just felt really uncomfortable.” Eventually, she deactivated her profiles and went off-the-grid, completely changing her online presence. Though 5 years have passed, she hasn’t reactivated several accounts for this reason, as information from one account could then lead to another.

“It feels like the world is closing in on you when you can’t get away from somebody and they continue to harass you and bother you and pester you, even though there wasn’t anything specifically violent.”

This is also why Emily never seriously considered reporting the incident, because she thought that the police nor anyone else would be able to do anything since the messages weren’t violent. However, the fact that the sender was continuously messaging her on various profiles violated her boundaries, especially as she was trying to cut off communication.

In the second incident, Emily was messaging someone on the dating-app Tinder, who insisted that she shared her phone number with them. When she explained that she wouldn’t do that until they met, the person sent an aggressive message claiming they had a right to her number and that this was essential for building trust. Emily told them she wasn’t comfortable and that perhaps they shouldn’t meet, at which point the person proceeded to send her rape threats and graphic messages.

“I was really freaked out, building on the last thing that happened, and also as someone who had already been raped as well. I think it was kind of jarring to get that.”

She cut off contact with the person but did not report them or talk about it with anyone besides her roommate. “I didn’t want to make it into a bigger thing.” There was also a general feeling of helplessness in terms of what official authority to turn to in such a case, something Emily always feels with online incidents.

However, this does not mean that the issue was resolved. In fact, Emily continued to feel unsafe in her everyday life because this person had seen her profile, could recognise her and had basic information about her.

“It just instilled that fear and uncertainty to be like: Will this person do it?, with how quickly the last person was able to find all my profiles, I know how easy it is to find things out about people. I don’t have a super high online presence but for the next few weeks I felt so aware. I feel constantly aware”.

The third incident occurred when Emily moved to a new country. The year prior, shortly after moving, Emily had been assaulted at a local bar, causing her to struggle even more with her mental health and feel unsafe in her new home. A few months later, Emily experienced another form of tech abuse when her colleague was being stalked. The stalker sent graphic and sexual death threats to Emily’s work email account in order to reach his target. This was extremely distressing. “I had this really big wave of feeling unsafe but also guilt, because I was telling myself, ‘you don’t deserve to feel unsafe, the emails aren’t for you.’ Opening your email inbox to that is terrifying even on the periphery, but the toll it took on the person they were meant for was life-ruining.” She also had to keep saving the emails because of the police investigation. Unfortunately, the police were also unable to provide any significant remedy.

“Seeing how little could actually be done to stop this was like the nail in that coffin. I’ve been shown how easy it is to be a target and how hopeless it feels to get justice. And even if you do get it to stop, that vulnerability doesn’t go away.”

In the long run, these incidents impact how safe Emily feels in both online and offline spaces. She reflects that jobs these days demand an online presence, even though it’s no longer something she feels comfortable maintaining. Emily feels that she shouldn’t be required to present certain information online. Instead, there should be greater emphasis on asking someone if they are comfortable sharing information, rather than assuming they will be.

“I spent a week and a half in an anxious panic because my job had asked me for a picture and a bio and I personally don’t feel comfortable sharing so much information online about myself,” she says. “I eventually had a conversation saying I didn’t want to do this. But it is difficult having to have these debates and thoughts in your mind, then having to be like I don’t want to be seen as difficult to work with. I don’t want to have to talk about this, but no one asks if you’re comfortable sharing these things and it is just assumed. When you do say you’re not comfortable you also feel obligated to give a reason why, or people will just make their own assumptions about what abuse happened to you.”

Emily is now healing and has access to therapy. She is learning to navigate through all these fears and emotions, has started volunteering to support other survivors, is thriving in her career and enjoys travelling. But she continues to struggle with her own feelings and fears surrounding tech abuse.

“I often think my response of feeling uncomfortable online is too much, and I should just get over it because it wasn’t even that bad. I think that’s a constant thought too. Which always just makes me more anxious.”

It is evident that the impact of tech abuse on her online and offline life remains profound.

“We’d have these conversations and it was almost as if he knew things that were going on in my life that I didn’t really know how he knew. It was a bit confusing. I had started seeing other people by this point, I was moving on with my life. He was being quite accusatory to me of things. I remember being like: what are you talking about? How would you know these things?”

Kate’s story

Kate was attending a university seminar when a text message from her ex popped up on her phone. It contained just two words: buckle up. At that point, she had no idea what the message was referring to, but she knew something was seriously wrong. What unfolded was a case of TGBV involving both cyberstalking and image-based abuse.

In 2009, Kate and her friends were travelling in Europe when she met Steven. He was Australian, and was on a year-long world trip with a group of friends. They were attracted to each other and hit it off, and kept in touch when Kate returned to Wales, where she lived with her parents. The relationship started to develop deeper as both of them visited each other in their hometowns and stayed at each other’s homes for several months on end.

Eventually, Kate moved to a different city to start university and the distance took its toll on the couple. She realised that it was a new chapter for her, and their long-distance relationship was not working. She called things off. At first, Steven was very upset, but they resolved to be friends and stayed in touch. However, their conversations became strange when it appeared that Steven knew more about Kate’s life than she was telling him.

Eventually, the communication turned extremely nasty and Steven started sending abusive messages on Facebook. Kate remembers feeling shaken, but also somewhat protected by the physical distance between them. She blocked him on Facebook:

> *“I remember thinking that this is really horrible, and it made me feel a little intimidated, but he was on the other side of the world so it kind of felt not as threatening as if someone was doing that who lived near you.”*

It was soon after this that Kate received that text telling her to buckle up. She immediately left the seminar, and then got a message from a friend saying something was going on with her Facebook account. Kate couldn’t access her account but by speaking to multiple friends, she pieced together what had happened.

Steven had hacked into her Facebook and was sending sexually explicit photos of Kate to her male friends. It was evident that he had been monitoring her account and new contacts, as he specifically messaged men that she’d recently become Facebook friends with. The photos were from when they had engaged in cyber sex, including screenshots that he had taken without her knowledge. He’d also hacked her email account and sent “a torrent of written abuse” to both her parents.

Kate called Steven and found him to be unrepentant: “He was completely defiant about it and was like: ‘this is what happens if you act like a sl*t.’” Kate remained calm and focused on regaining control of her account. In the meantime, a friend contacted the men who received the pictures to tell them what was going on, and asked them to not look at the images and delete them immediately. After a few days, Steven gave Kate the password to her account. The first thing she did was report the abuse, but to no avail. She then ended up deleting her account:

> *“This was back in 2011. There really wasn’t any mechanisms in place to report stuff like this. I didn’t even get a response. Nothing happened.”*

Kate recalls feeling intense humiliation, shame, anxiety and stress as a result of the abuse. Telling her parents everything was particularly difficult, but she was thankful that they, along with many of her friends, were very supportive. Kate resolved to move on with her life, and she did, but the impacts of the experience lingered:

> ***“It was definitely this kind of shameful thing that I felt like I was carrying around with me, particularly at university.”***

The incident also impacted how Kate uses the internet. She describes herself as someone who is “very invisible online.” Although she made another Facebook account after deleting the compromised one, she didn’t have it for very long. In fact, she now has very few online profiles, and those she does have, such as LinkedIn, don’t have a photo. This limits her ability to support causes or issues she cares about online but she comments:

> *“I don’t want to have any public profile that could put me at risk of further humiliation.”*

In 2011, when Kate experienced image-based abuse, it was barely known or spoken about. While there is more awareness and discourse regarding this form of abuse now, it seems as though the issue is getting worse. Kate is appalled that so many women are still going through what she did:

> *“It’s a total violation. You do feel violated. That for me is what makes me angry. So many women feel violated. All they’ve done is maybe break up with a partner. Everyone has the right to break up with someone! Now it’s become a lot easier for men to take their anger or shame or whatever it is they feel in response to this and really damage a woman. And it can have long-term impacts. Not only on how she feels about it but on how other people perceive her…I’m always open or vulnerable to being blackmailed now. That’s how I see it.”*

3 How systems are failing survivors

Survivors of tech abuse are consistently failed by the institutions, authorities, and systems that should protect and support them. The challenges survivors face when trying to access support can cause further harm to them, including within our three fields of interest: tech, research, and policy.

Often, technology is designed without considering how it may be used to cause harm and, as a result, has inadequate or non-existent safeguards and support mechanisms. Technology design often replicates the systems of oppression of wider society and amplifies existing inequalities, and reporting and remedial processes are often inadequate, inaccessible, and retraumatising. Research can be a retraumatising site for survivors of abuse, as it is often carried out in extractive and harmful ways, where the survivor is expected to recount their trauma with little support or information about how their testimony will be used. Policies on tech abuse are also insufficient. In many cases, the policy landscape has simply not kept up with the pace of new technologies. Even when policy does exist, it can use vague language that may end up victimising survivors (such as laws that may criminalise consensual sharing of intimate images) or take a narrow approach which excludes the experience of marginalised groups (such as defining intimate images too narrowly). Again, survivors are often left retraumatised by the justice process.

Ultimately, all of these system failures point to a lack of intersectional, survivor-centred, trauma-informed approaches. This facilitates the continuation of tech abuse, as without this lens we lack sufficient tools to counter the harm.

3.1 How technology enables abuse

There are several features of tech platforms that enable or facilitate tech abuse. While these features are not designed for abusers – they are usually designed for other, valid reasons such as user experience or efficiency – these vulnerabilities can be easily exploited to cause harm.

Vulnerabilities common to many tech platforms include:

- **Limited user choice in what information is made public:** Most social media platforms make some personal information publicly available, which can be used by perpetrators to identify, harass, and stalk survivors.

- **Applications connect contacts from phone, email, or social media and alert them:** Many platforms auto-upload contacts from users' phones or other social media accounts to allow people to quickly find friends and acquaintances already using that platform. This can enable abuse by automatically reconnecting survivors with their abuser and/or giving perpetrators frictionless access to many contacts. Some platforms also send alerts to users whenever a contact joins a platform, furthering this problem and the risk of triggering survivors.

- **Frictionless sharing of photo and video content:** Most platforms allow

easy downloading of photo and video content, making it easy for perpetrators to save, share, and use content. In addition, most platforms allow users to take screenshots of others' content and/or conversations without notifying the user.

★ **Sharing enabled for external applications:** Many platforms also include features for quick and easy sharing from one app to another. This feature can be used to easily spread abuse.

★ **Rigid and hard-to-find privacy settings:** While most platforms do offer a variety of options for privacy, these are often inflexible and do not allow people to personalise their privacy preferences. This means survivors are torn between risking their safety or completely privatising their account, which might have other professional or social consequences.

★ **Anonymous accounts:** Anonymous accounts are important for survivors and other marginalised folk. However, they can also be used by perpetrators to carry out abuse without accountability or consequences.

★ **Slow and not fit-for-purpose moderating and reporting mechanisms:** Across many platforms, the tools and processes to report abuse are not easy to find or use, are often slow, and may not be available for some languages at all. Furthermore, algorithms frequently fail to flag abuse, even when it's reported, and when human teams are working on abuse reports, they can fail to recognise and appropriately deal with abuse due to a lack of training and context-specific knowledge. This issue is particularly pertinent in the Global South, as without sufficient cultural knowledge and training, moderators often do not recognise abusive content as abuse.

> *"People who complain using the reporting mechanisms find that they don't get a reply. It just sort of vanishes. There is no information on what is going to happen etc. There is a complete lack of transparency and that is one of the issues. A complete lack of response."*
>
> Bishakha Datta, Point of View

★ **Lack of timely, appropriate, and culturally adaptive moderation:** Inadequate policies and training of content moderators can create lags and lead towards incorrect decisions that harm survivors.

★ **Harm through content moderation:** Content moderation is often outsourced to poorly paid and supported 'ghost workers', usually based in the Global South. Reviewing abusive content can be traumatising, yet these workers are not given sufficient training or psychological support. This extends, rather than mitigates, harm.

★ **Being able to contact people without pre-approval:** Platforms that allow users to call, message, and nudge people they do not know, without any options to set or change this preference, makes targeted harassment easy.

- **Ability to create large distribution groups:** This makes room for rapid dissemination of abusive material, such as intimate images.

- **Keeping users logged in even though they may be on a shared device:** For ease of access, many platforms offer default settings which keep users logged on to their platforms unless they proactively log off. This creates several security risks, including tech abuse.

- **Limited recognition of the safety needs of people living in countries with oppressive regimes:** Political dissidence or protesting restrictive reproductive rights can be a lot more dangerous for women in countries with oppressive regimes, leading to imprisonment and sanctioning of activists. Women and queer activists are often targetted with dangreous gendered misinformation, dealth and rape threats, and doxxing which can pose a risk to their lives. These platforms are vital places for activists to mobilise their communities and share their work, and therefore their safety has to be ensured.

- **Lack of blocking and muting options:** Different options for blocking and muting have evolved in recent years. For a long time, this was not possible on Twitter, Slack, and Skype.

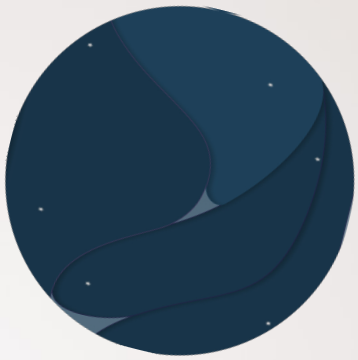
Certain tech products also have specific vulnerabilities. For instance, iCloud makes it easy for perpetrators to take over multiple devices and access content, contacts, and more. Snapchat maps enable and encourage the sharing of location data. Facebook groups are used extensively to coordinate abuse. YouTube hosts channels for perpetrators seeking advice, guidance, and techniques to help them abuse. Reddit houses threads which illegally share content from OnlyFans. Clubhouse's onboarding process meant survivors were notified when their abusers joined the app, and both Clubhouse rooms and Twitter Spaces have created platforms for defending abusers and misogynistic speech. Up until late 2021, Google Drive did not allow you to block users, which meant abusive people could keep sharing files on Google Drive and it would still show up on 'Shared with me'. Features such as 'story views' on Instagram and 'viewed your profile' on LinkedIn can be used by stalkers to communicate that they are watching, while LinkedIn may be used for workplace harassment, as it normalises sending private messages to work contacts or colleagues.

In addition to direct abuse, several platforms have censorship policies and practices that disproportionately harm marginalised groups and those campaigning for social justice, which can serve to reinforce systems of oppression and stall progress on issues such as GBV. For example, 'shadow banning' on Instagram and Tiktok is when a person's content is not shared with their follows, but they are not informed or given reasons for it. As Safiya Noble has argued in Algorithms of Oppression, even search engines can facilitate harm by embedding biases against women of colour into their algorithm and search results.

Messaging apps also facilitate abuse. The default setting of messaging apps like WhatsApp and Telegram is to show when someone was last online, which can be used to track survivors. The accessibility and anonymity of these apps make them prime platforms for perpetrators. Group chats and the

forward function are used for rapid dissemination of abusive material, and it's easy for users to make new groups when old ones are deleted or if they are removed from them. Privacy features of Telegram in particular, such as heavy encryption and auto-deleting messages, are widely abused to perpetuate TGBV. On Skype, users can message, call, or video call others to harass them without even being added as a contact.

These are just some of the many vulnerabilities in tech platforms that can be exploited by abusers to carry out TGBV. These features have not been designed to facilitate abuse, but they do. The vast number of tech vulnerabilities shows the failure to consider and mitigate tech abuse in regards to tech design.



Case Study:

Electronic Frontier Foundation - Stalkerware and Apple AirTags

Electronic Frontier Foundation (EFF) is a USA based non-profit that works on ensuring civil liberties in the digital world. They champion user **privacy** and freedom of speech and expression, alongside technology development that supports global justice and innovation.

Apple launched the Apple AirTags on April 30 2021. These were marketed as small, inexpensive trackers that can be attached to or slipped into your belongings, so that you can keep track of items like keys or wallets. An iPhone is paired with the owner's AirTag so that they can play a sound on the AirTag or use its geolocation to locate any items they've attached it to. But AirTags can be used nefariously - they can easily be slipped into someone's bag and used to stalk them.

EFF was quick to recognise and draw attention to this risk. By mid-May, Eva Galperin, Director of CyberSecurity, wrote in Wired about these concerns. Apple AirTags are especially of concern in situations of intimate partner violence, where the domestic abuser could easily slip an AirTag into the survivor's bag to track them. This issue is not unique to AirTags, and is equally applicable to other tracking devices, such as Tile. However, Apple has a huge network, which means AirTag is able to show accurate locations by connecting with the Bluetooth of every active device in the Apple network. All Apple devices are added to the tracking network without first asking for the consent of Apple users. While it is possible to opt-out, users must do this for each device they own.

There are two safety features for iPhone users: a notification popsup when an unidentifiable AirTag is nearby, and nearby AirTags can be viewed through phone settings. However, initially, Android users had no way of finding out if there was an AirTag on them. Though AirTags have a serial number printed on them, which can help with finding out who owns it, it's difficult to locate the device on you in the first place as they are deliberately inconspicuous. The only safety feature built within the AirTag was that after 72 hours of being separated from its owner, it would ping at 60 decibels to alert those nearby. Since the sound isn't very loud, this could easily be muffled by placing it between things. According to Galperin, it's also unclear how long the beeping goes on for, and as she pointed out in Wired, 72 hours is a long time. This causes a huge safety concern for the person being stalked, especially if they live with their abuser, who can easily reset the alert every 72 hours. If they don't live with them, it means a person is still being stalked for 3 days without being alerted.

> *"When Apple fails to protect survivors, the consequences can be fatal. Apple leadership needs to give abuse survivors and experts a central place in its development process, incorporating their feedback from the start."* - Eva Galperin

With Galperin's help, journalists at The Washington Post also wrote about the issue, testing the device out in June. EFF proposed that Apple should design an Android app to alert users about Apple's AirTags. In June, Apple decided to change their policy and reduce the time it would take the AirTag to beep, from 3 days to 8-24 hours. In December 2021, Apple launched Tracker Detect, an Android app to help users identify if an AirTag or any other Find My Device is near them. The app shows nearby AirTags as an unknown item and can play a sound within 10 minutes of finding the AirTag. This is a major improvement from Apple, and is a direct result of EFF's advocacy. However, unlike the iOS app, the app won't run in the background and automatically alert the user. Tracker Detect requires that the user opens the app and runs a scan for the devices. The app will then provide instructions on how to disable the AirTag.

While there has been progress, safety concerns remain: the sound of the AirTag alert is still low and innocuous, the Android app isn't issuing alerts, and there's the issue of the alert being reset by an abuser who lives with the survivor. While Apple safety features are generally stronger, Apple users have to rely on the company's automatic scanning and have no way to actively scan, which can be an issue if you're tracked over a short trip. There are also loopholes such as family sharing, where family members can turn off the alerts on the device, or an abusive partner can simply tether the AirTag to the survivor's own iPhone so that they don't get any alerts. In 2022, Vice, the Guardian, the BBC, and others reported on rising cases of AirTags being used for stalking across the USA. Apple is continuing to introduce and investigate new safety features.

Our principles in practice

Though Apple has to be given credit for recognising the need to change their decisions, the case study provides us with a chance to reflect on what went wrong in the design process. When The Washington Post asked Apple if they'd considered domestic abusers and stalkers in their research, they were evasive. In Galperin's assessment, had they consulted an intimate partner violence specialist or survivors, the device design would have been very different from the start. Thus, Apple did not properly consider **safety** concerns when launching the product. Very overtly so, by enabling stalking, an AirTag completely infringes upon survivors' right to **privacy**, though it may very well maintain the **privacy** of the stalker who owns the device. EFF proposed that Apple users should not be automatically added to the tracking network, but should be able to give their consent, because it also makes all Apple users enablers for the stalker or abuser.

EFF also suggested that by giving space to experts and survivors of abuse, and involving them in the design process from the beginning, Apple could come up with better **safety** features for their devices. This would begin the process of **power redistribution**. Furthermore, the initial discrepancy in how Apple users were notified of an AirTag while Android users were not, showed a lack of **plurality** in the design of the device. The cost of having a mobile phone and the price difference between Android and Apple meant there was a class disparity in who this issue would affect, as it would particularly impact lower-income women and those in the Global South.

This posed major **equity** concerns. By addressing this through an Android app, Apple has demonstrated **accountability** for the harm their product decisions can cause. However, concerns remain, given that the **safety** measures for Apple and Android devices are still unequal, and very limited for those without a smartphone.

Galperin and EFF continue to advocate for survivor-centred approaches to eradicate stalkerware.

A systemic problem

Other than the features of tech platforms that are exploited to perpetrate abuse, there are systemic causes and structures that create favourable conditions for abuse to flourish and lead to inaction from tech companies. While these foundational issues are not the focus of this guide, they must be acknowledged as they underpin how and why technology facilitates abuse.

Prioritisation of issues and regions: Addressing tech abuse is not a priority for many tech companies. As tech abuse has gained more attention in recent years, more resources and efforts have been dedicated to tackling it, but this effort remains negligible in comparison to the gigantic turnover of these platforms. The problem is exacerbated by market prioritisation: there are unequal responses to tech abuse and thus different experiences for survivors between different markets, depending on economic priority. In particular, there is a huge discrepancy between the Global North and South, which manifests, for example, in the lack of proper reporting mechanisms in languages other than English.

'I think they are actually deciding not to invest in this. I mean, it's not that they are not capable of it, it's that they are deciding not to. They have all the resources. They have financial resources, artificial intelligence resources, they have offices all over the world. They could really be making the difference, and I think it's just that the priorities are not there.' - Lulú V. Barrera

'All tech companies have priority markets, where they know they have a presence, it can influence other behaviour in a specific sub-region. So that also means that the priority of issues or the priority of solutions go to those specific markets, they just don't trickle down to everybody. I remember once attending Facebook launching a missing child alert in South Africa. And I was wondering, when is it going to roll out to the other countries?'' - Chenai Chair, Mozilla Foundation

Business model: The business models of most social media platforms are built on engagement, whether that is driven by civic or hateful speech. The more people engage, the more profit tech platforms make. Arguably, this business model is incompatible with effectively tackling tech abuse, because it is not in the interest of tech companies to curb abuse as long as it is driving engagement.

'I would say the major problem with social media platforms when it comes to this kind of abuse is that, for most of these companies, their entire business model is in engagement. It doesn't matter what kind of engagement. It doesn't matter if that is good or bad, or destroys someone's life, it's just the more you get people to engage, the better it is for the company. When that is your entire business model, you don't prioritise things like harm, and you don't prioritise things like keeping people safe, you just prioritise having more people engaged.' - Mary Anne Franks

Power asymmetries: As tech giants grow and increasingly monopolise sectors, the power asymmetry between them and citizens, as well as civil society and even governments, increases. The use of technology has become a point of access to more and more vital services, leaving users with nowhere else to go, and no power to reject or question their terms of use. Tech companies wield power over governments by offering relevant tech infrastructure, as was demonstrated with the development of the COVID-19 contracting tracing apps, and Google and Apple's decision to integrate the technology into their operating systems. Tech giants have become too big to fail.

Diversity within teams and leadership: The inequalities of the wider world are often mirrored within tech companies, and discrimination is a major issue. While diversity and inclusion of marginalised groups is an issue in tech at all levels, it is particularly so at decision-making and leadership levels, meaning the concerns of marginalised groups are easy to ignore. The lack of gender diversity in tech - only 20% of the USA tech workforce is made up of women - is especially detrimental when it comes to tackling gendered tech abuse. Worryingly, AI may make this situation even worse, as women are at higher risk of displacement by automation than men.

3.2 When research creates harm

There's no dearth of research on GBV. Early records go back to the beginning of our understanding of human psychology. Unfortunately, harmful practices in research settings have a long history, too. For example, psychologists and physicians such as Sigmund Freud ignored women's experiences of sexual abuse in hysteria studies in the 1800s.

Though research methods have changed over time, ethical considerations about how trauma is studied, believed, portrayed, and extrapolated into findings remains highly relevant today. The term 'extractive research' is used to refer to research where information or knowledge is 'extracted' from those with experience or knowledge of the research subject without care or interest in their wellbeing, preferences, and needs.

In regards to GBV, research is extractive when it uses the experiences and labour of survivors without appropriate consent, control, or compensation. This might involve reducing a survivor's role and input to that of an informant, disregarding pain or discomfort that may be caused by participation in the research, or discarding information that dissents from the organisation's own ideas.

Issues of extraction are particularly pressing in a global context. Firstly, many international research projects are shaped by geopolitical power dynamics and colonial history. Annie Bunting and Joel Quirk have written about considering ethical research practice when studying GBV in African conflicts; they say, "the French, Portuguese and British continue to play major roles in producing knowledge about their former colonies, contributing to a larger pattern which involves privileged outsiders parachuting into 'exotic' locations for short 'fact-finding' expeditions." At the same time, zooming out to look at the overall research landscape shows staggering inequality in what research is funded, who produces it, where it's produced, and whose research interests are prioritised. When survivors' insights are treated like an asset but their own agency in the process isn't, when they are consulted but have no idea of why and how their experience will be used, and when language, culture, race, disability, and other characteristics aren't considered even when survivors mention them, it's extractive.

"Harmful research methods are basically extractive research methods where with that quantitative data side you go in, you collect the information then you come out and go and give it to someone else and don't give it back to the community that participated in it.

The politics of research means that someone who's based in a university in the UK or US would be comfortable to name the issues of violence against African women. So there's that power dynamic within the research space that makes one feel like they can write about and on these particular groups of people without really engaging with them." - Chenai Chair, Mozilla Foundation

In the case of researching GBV, or any other form of trauma, a further concern is 'retraumatisation'. While there are various definitions of retraumatisation, and the term is not clinically validated, it is widely used to refer to instances when an experience causes a survivor's negative feelings of trauma to reemerge. As holocaust survivor Primo Levi has written in *The Drowned and The Saved,* "the memory of a trauma suffered or inflicted is itself traumatic because recalling it is painful or at least disturbing." If special care and attention is not given, research can end up being a painful experience for survivors which reignites past hurt and emotions. Retraumatisation can occur when interviews force survivors to disclose trauma in gory detail though there is no need for it, or when questions aren't asked with the understanding that trauma might elicit leading responses.

> *"Gender-based violence research is actually quite traumatic. So I'm always wondering what are the safe spaces for the people who do this research?"*
>
> *Chenai Chair, Mozilla Foundation*

A further issue is vicarious trauma, where those doing the research experience trauma through exposure to and engagement with the subject matter. Through consistently engaging with traumatic content, researchers can themselves experience trauma symptoms and negative emotions, especially if they have a personal connection to or experience of what they are researching. This is an especially pertinent issue when it comes to GBV, as its ubiquitous nature means that many researchers will have direct experience of it. When the possibility of vicarious trauma is not considered and mitigated, researching the issue can extend rather than address trauma.

Just because we can ask something shouldn't mean we have to. Just because we can record audio doesn't mean we should hold on to it for years. The research team and, where relevant, commissioning organisations are responsible for reducing the likelihood of extraction, retraumatisation, and vicarious trauma.

User Research

In both the product and policy design worlds, there has been a move towards more robust, evidence-based models. As a result, user research has emerged as a flourishing field and profession. It seeks to understand the behaviours, needs, and motivations of users or potential users of any product, service, or policy. In the non-profit space too, many funders require organisations to validate their hypothesis about user behaviour with research methods such as surveys, interviews, and personas. This development is encouraging, but extractive and retraumatising practices still remain a concern.

In the technology sector, there is one particular methodology of user research that has been considered ground-breaking and has had substantial traction. The launch of the Human-Centred Design (HCD) toolkit by IDEO in 2009 brought a wave of change in the way academics and researchers approached subjects like poverty, abuse, and unemployment. This shift rapidly put more agency in the hands of the interviewees and soon, they were co-producing rather

than passively engaging in research. The principles of human-centred design are to encourage open and non-leading questions to help understand the needs and lives of people we're designing for, improve ideation, and lead to more productive and creative idea prototypes. HCD provides a toolbox of more than 150 design techniques and tools, including personas, experience maps, and empathy maps. It has become the methodology of choice for most technology and public policy companies and is largely considered as best practice, so we're going to focus on it here.

HCD undoubtedly did tackle and respond to many of the limitations of traditional research. However, it is not without its own limitations, especially when applied to gender-based violence without an intersectional, survivor-centred, and trauma-informed lens. As Tania Anaissie, a design thinking practitioner and lecturer, critiques, "it exacerbates power asymmetries, that it pretends to be apolitical, that it ignores the complexity of systems, and that it does not hold designers accountable for the impact of their work."

Indeed, many women and people of colour who worked for IDEO and were swept up in this wave of HCD-led transformation have written about their negative experiences with the organisation, highlighting their disillusionment with the methodology.

Given HCD's predominance in the technology sector, it is worthwhile to understand where and why it is lacking. There are several important criticisms of HCD, many of which apply equally, if not even more so, to other forms of user research.

1. Favours generalisation and oversimplification

Personas, experience maps, and surveys are especially prone to this. The tools themselves do not present the limitation, it's the assumption that a group of humans can be reduced down to a snippet of their lives. It's what Nigerian feminist and author Chimamanda Ngozi Adichie calls "the danger of a single story". In her TED Talk she explains, "The single story creates stereotypes, and the problem with stereotypes is not that they are untrue, but that they are incomplete."

These are just some of the errors that can make their way into our work:

★ Out-group homogeneity bias: Where we see our community as diverse but an 'out-group' (a group that feels different) as being homogenous, or unvarying.

★ Fundamental attribution error: Where we believe someone's actions are because of their character (something in their control) and our actions are based on external factors (not in our control).

★ Confirmation bias: Where we seek, interpret, and remember information that confirms our beliefs and opinions.

2. Doesn't prioritise safety

When we research traumatic pasts and presents, it is natural that our research intervention will be difficult for some people. This includes the researchers themselves, especially if they've had experience with similar issues. While we cannot prevent the emergence of these emotions and memories as they may be related to

memories as they may be related to our subject area, we can acknowledge them and plan for them. Human-centred design approaches often miss this because they believe co-production is enough to negate these emotions, and researchers should be able to manage their own emotional safety because they have to.

3. Ignores or worsens power asymmetries

IInformed consent is a cornerstone of ethical research, and HCD is no different. Consent forms are a critical part of the administration, but researchers often do not go far enough to explain the purpose of research, why they need consent, and when people can opt out.

This becomes really important when there are power asymmetries - financial, social, or political. Due to historical abuse by people or institutions, many people may sign consent forms simply because you've asked them to and they're used to doing that.

Reasons why someone might not opt out even when they want to:

- ★ Politeness: Someone might feel it's too awkward to opt out as they do not want to embarass you or appear rude.
- ★ Financial: They really need the money and think they won't get the compensation if they opt out (if people take part in the research, they should be partially or fully compensated irrespective of what stage they drop out of).

To build and honour trust, we need to make sure the people who are aiding our research with their stories truly understand the intent and process through which their pain and experiences will be treated.

4. Assumes neutrality of the designer and design processes

Some research should not be done because there is a possibility to perpetuate harm through incomplete, superficial, and biased research. Systems design doesn't acknowledge historical trauma and structural oppression.

Research often assumes neutrality of the designer and design processes but we know that is far from being true. Our privilege and affiliation with institutions, which may have a history of cultural blindness and discrimination, can introduce so many visible and invisible harms. This is further supported by the 'toolification' of user needs, which isn't being viewed as a framework to investigate needs, and has instead become a lazy template for generalising complex circumstances.

Sometimes 'empathy' can end up being misguided and ultimately harmful, when researchers seek to 'empathise' with experiences they do not know first hand. Ableist and offensive approaches include instances where designers wear crutches and blindfolds, and walk around for a few hours to 'understand' what life is like for users, or when they

create virtual reality games to immerse people into a new experience. Instead, these research methods are often celebrated as breakthroughs and given public acclaim within the research community.

"We teach designers that they can tap into empathy to design for communities that aren't their own, or for people whose lived experience they don't share. And we see this a lot, we see designers who are trying to improve some part of the disabled experience by walking around blindfolded or walking with crutches, instead of actually centering the lived experience of people with disabilities. As a designer, I'd rather you show me the practices built into your design process that focus on improving the material conditions of the people you engage, making sure that they are compensated, that they are treated well, that their wellbeing is a priority for you, that you're actively countering dominant behaviours in the way you work with them, that you're giving them opportunities to make choices for themselves."

Sarah Fathallah, independent social designer and researcher

5. Short lived processes without followups

Some research should not be done How do you support the adaptation of your prototype to a changing environment? Shiny prototypes, especially if they require high-resources in a low-funding context, will evidently die out when the volunteer time of dedicated people burns out or when the energy of funders who like new things fizzles out. HCD believes in continuous improvements, but if pilots or preliminary research stages are set up without the realities of resources and leadership sustainability in mind, there's a good chance the project might fail.

Overall, it is clear that for all the progress that HCD has brought to the research field, there remain several, serious shortcomings, especially when applied to an area of research as sensitive as tech abuse. For all its advantages, it still has the potential of creating research environments that feel one-sided and extractive, leaving survivors feeling powerless. The need for more trauma-informed, intersectional, and survivor-centred approaches to research remains crucial.

3.3 The pitfalls of policymaking

"Many people who face harassment on social media try to use the reporting mechanisms and I've yet to hear of a successful case. That's been one of the big challenges. Very, very few women that we know actually turn to the law or actually file a police complaint, because of so many barriers with the law. "

Bishakha Datta, Point of View

Policies to tackle tech abuse are often drastically inadequate. Here, we are focusing on 'big p' policy - the criminal and civil laws that focus on survivors and the regulations targeted towards the private sector. Policies which

address tech abuse often fail survivors from inception to implementation.

Some countries have no stand-alone legislation to address the different forms of TGBV, meaning existing laws have to suffice. For example, the UK has only recently proposed criminalising cyberflashing, among other harmful acts, in its new Online Harms Bill. Similarly, in Bangladesh there is no specific legislation addressing image-based abuse. Instead, there exists a confusing patchwork of laws that makes it complicated and difficult for victims to seek justice. Some countries have laws that do little to tend to the needs of survivors, while others have laws that are actively harmful. Even where laws and policy do exist on paper, they are often lacking in scope, depth, and nuance. Frequently, they are too narrow: they focus on the specific type of abuse while ignoring the larger context and impact it can have. For example, the Cybercrime Prevention Act of the Philippines has been widely critiqued for incorporating badly-defined, vague, and overboard elements which ultimately put women at risk. In India, the Information Technology Act does criminalise IBA, but anyone who sends an intimate image depicting sexual conduct can be caught under this law, including people who consensually send images to their partners, putting them at risk of being prosecuted. Similarly, East Africa's new anti-pornography laws have ended up with victims facing prosecution instead of those who stole the images. Such laws not only deter reporting of abuse but they often imply the idea of 'public morality' which further leads to victim blaming.

At times, the law also excludes considerations for those who are most marginalised, such as migrant or traveller communities, sex workers, and LGBTQ+ individuals. The plurality of survivor experiences is frequently neglected. Even governmental or other organisational bodies that are created specifically to respond to tech abuse often have gaps in their understanding which limits the types of online harms, age ranges, and communities they will consider supporting. This leads to inconsistencies between what is recognised by law or policy and the diverse ways in which survivors of tech abuse experience that law or policy in practice.

Policy is lagging behind

Given the ever-changing and accelerated pace of technology, policy often lags significantly behind when it comes to properly defining tech abuse in its many forms. As tech has developed over the years, it has been evident at every milestone that it can, and likely will, be used to cause harm. From email messages leading to incredible levels of spam and social media posts leading to online violence, hate, and text-based abuse, to the unprecedented use of video calling during the pandemic leading to 'Zoom bombing' difficulties - the law simply hasn't been able to keep up.

Instead, survivors and those trying to support them are often made to navigate a complex web of copyright, IT, criminal, and other laws. More recently, there has been an emphasis on trying to align laws and regulations globally, in particular at the G7 Summit in 2021, but this has not yet come into fruition. The lack of regulatory consistency across borders also allows tech companies to act with impunity when it comes to tech abuse and makes it difficult for survivors to

appropriately have their complaint addressed when harm does occur. It also offers more loopholes for perpetrators to evade the law and take advantage of different levels of regulation in different countries to perpetrate harm.

The risk of miscategorisation also occurs when those who are responsible for implementing the law wrongly classify a harm in a manner that downplays its severity, legal consequences, and/or impacts on the survivor. When instances of abuse occur, such as image-based sexual abuse, online harrasment, or use of deepfakes, law enforcement authorities are still often unsure how to categorise or report it, meaning survivors are unable to seek the redress they want. For example, law enforcement sometimes categorises these forms of TGBV as tech crimes rather than gender-based violence, thus minimising the state's response and preventing provision of a holistic and compassionate response to survivors.

Excluding those at the margins

Laws, policies, and justice processes related to tech abuse, where they do exist, tend to apply one-size-fits-all definitions and rules. When policies fail to take stock of the different lived realities of survivors, and ignore aspects of people's identity such as gender, sexuality, race, national origin, class, and age, they end up treating the dominant social group as the standard around which laws are crafted, making it particularly difficult for marginalised groups to access justice. Since many of these communities are already heavily policed or criminalised, they are left without any adequate recourse.

For example, most policies do not specifically account for the experiences of LGBTQ+ people who experience 'outing' of their sexual orientation or gender identity publicly. Doxxing policies tend to address the issue of publicly leaking private information, such as name, contact number, email address, and home and office address, but do not include the act of 'outing' someone. Similarly, sex workers, who are already criminalised in many countries, are inadequately protected from individuals who steal their content (which is often behind a paywall) and upload it onto free sites, making profits by reselling it or using it to harass sex workers.

In some countries, overbroad laws criminalise free sexual expression and bodily autonomy with devastating impacts on LGBTQ+ people and young people in particular. Such overbroad laws can lead to the criminalisation of survivors themselves, for example, for sharing intimate images. This may particularly impact individuals who use sexting to be intimate due to cultural or social barriers that make in-person contact impossible. Such laws end up criminalising free sexual expression, rather than focusing on the real harm - the violation of consent. Alternatively, Florida's 'don't say gay' bill is an attempt to ban the discussion of gender identity and sexual orientation in classrooms all together.

Some countries, such as India, also have laws that police indecency and women's 'modesty', and are rooted in deeply patriarchal notions. Such laws rely on a morality-laden discourse that tends to shame sexuality, thus further contributing to victim blaming. This leads to online spaces being increasingly controlled by the state and free expression by people

of marginalised genders viewed as indecent, vulgar, or worthy of prosecution. In the USA, some states do not have a way to distinguish abusive sexting from consensual sexting when a person is a minor and this often results in the victim of a privacy violation being charged with the possession and distribution of child pornography. When victims are categorised as criminals, they are not able to access victim support services because in the eyes of the law, they are not seen as victims, but as perpetrators. When victims do not have access to services like Victims Compensation or therapy, they are at higher risk for engaging in harmful coping mechanisms, such as substance abuse, eating disorders, and self-harm, while also dealing with the long-term impacts of being a court-involved youth.

Barriers to reporting

For survivors who seek justice, a significant barrier is the retraumatisation caused due to the reporting and justice process. From victim blaming and lack of privacy, to rigid sentencing frameworks focused on criminalisation instead of justice, survivors face a range of issues.

For instance, survivors may hesitate to approach the police for fear of being shamed or dismissed. Research has shown that police have failed to take tech abuse cases as seriously as physical abuse. For example, survivors report that police officers often tell them to simply change their number or block someone, instead of offering a meaningful remedy. Further, practitioners and survivors describe police to be lacking adequate understanding of the law and technology, often lacking financial and technical resources to investigate, engaging in victim blaming, and encountering evidentiary challenges, including identifying anonymous perpetrators. Survivors from marginalised groups are often even more hesitant to report crime to the police for multiple reasons, ranging from prior negative experiences with the police to language barriers, lack of legal aid, or insecure migration status.

There are also often very low levels of confidence amongst specialist support workers to help survivors of TGBV. Historically, frontline practitioners are exceptionally skilled in addressing physical safety concerns and managing how to mitigate risk, but less well equipped to support digital concerns. Without a robust support system, survivors' confidence in approaching police or other services, in giving evidence, and in finding non-criminal justice support options and mitigations is dramatically reduced. The hope that there is an organisation who can offer substantive help all but disappears.

Separately, the failure of court systems to ensure privacy and anonymity in many tech abuse cases is a major barrier to survivors' likelihood to report. In the USA, for example, there is a strong tradition in favour of litigants using their real names in civil suits, and federal courts generally require judicial consent before a plaintiff can proceed under a pseudonym. In criminal proceedings, most states in the USA do not guarantee that the survivors' identifying information will be kept confidential, including on court transcripts. To protect survivors, lawyers can opt for varying options at the state and federal level. However, even the fear of lack of anonymity can impact survivors' mental health, employment prospects, and personal relationships.

This general failure is compounded for marginalised communities. In the UK, for example, the Law Commission noted in its 2021 report that the lack of anonymity is especially devastating to LGBTQ+ survivors who may be 'outed' due to the proceedings. Likewise, individuals from specific religious or cultural backgrounds may also face expulsion from their families or communities if the nature of the harm becomes widely known – especially if the perpetrator is from the same community.

Lack of corporate accountability

Tech abuse inevitably includes more than one party. Besides the survivor and the primary perpetrator, there are often many more actors involved. Most countries do not have the legal mechanisms to hold technology platforms, website hosts, or downstream distributors (those who repost or redistribute the image) accountable for the abusive content they may be hosting or sharing.

Legal systems tend to look at tech abuse as an individual instance of harm rather than a systemic one and thus leave it up to platforms to find a solution. One of the ways in which this can place undue burden on a survivor is to make them responsible for removing their own images or private details from the internet. Most tech companies have at least some internal policies and procedures to support survivors, but without adequate regulatory or policy support, it becomes difficult to hold them accountable or make them bear the burden of investigation and justice.

The limits of carceral responses

Emerging research suggests that criminal responses to tech abuse do not adequately address the central needs of many survivors nor do they account for the diversity of harms that exist in many of these cases. An intersectional approach to survivor-centred justice for tech abuse recognises that a 'one-size fits all' approach does not work, and that justice must be individualised. This calls for a wide range of options, including non-criminal processes and acknowledgments of the harm.

Criminal law and carceral approaches can have significant limitations in terms of preventing such abuse from reoccurring in the future, especially when it comes to already marginalised populations. Therefore, it is vital that other paths to justice, healing, and accountability are explored in parallel.

Replicating offline systems: In many ways, the online world replicates the systems and social norms we see offline. Therefore, sexism, heterosexism, transphobia, racism, and other systems of oppression will show up in our online worlds as long as they continue to exist in our offline worlds too. This means that our work requires us to dismantle those systems, however they show up, including within law enforcement authorities and the criminal legal system itself.

Capacity and suitability of the criminal legal system: It is being widely recognised that the criminal legal system and prisons are not fit for purpose when it comes to deterring further harm. Research in the USA shows that long prison sentences have little impact on crime and can often make someone more likely to commit crime in the future. Ultimately, we need to consider how to create sustainable mechanisms towards accountability, justice, and freedom. Consider what it might mean to move away from carceral approaches to harm and instead organise community-based responses and interventions to combat forms of violence.

Abuse of power: There are also concerns that relying solely on increased criminalisation to tackle TGBV may actually increase surveillance, censorship, and control by the state and/or corporations. This will ultimately endanger the rights of individuals, especially those who oppose or criticise their governments.

Re-centering the survivor: Currently, courts often fail to acknowledge the harms of tech abuse. For example, in the case People v. Barber in the USA on image-based abuse, the court in its judgement stated that naked photographs were posted on Twitter and sent to the survivor's employer. However, there is no consideration of the impact, whether loss of employment or emotional distress, in its final decision. A lack of focus on the impact on survivors means that remedies are sorely lacking and do not respond to the needs of survivors. Therefore, it is worth considering whether other non-carceral processes could do a better job of centering survivors' needs and experiences.

While it is out of the scope of this guide to delve deeply into all the possible alternative approaches, individuals and community groups have started to take up that challenge. Some are looking at "holistic, relational, and flexible responses," especially when it comes to young people and schools which focus on relational and restorative approaches such as community circles, in hopes of institutional change and individual accountability. Others are discussing the potential of community-based responses when the 'community' is global and online. HeartMob is an innovative example of how online communities can support people experiencing online harassment by empowering bystanders to act. Elsewhere, organisations like Creative Interventions have developed tools for alternative approaches to violence, which could potentially be adapted for TGBV as well.

Case Study:

The Law on Image-Based Abuse

The nature and scope of laws that address image-based abuse (IBA) varies around the world. Some countries have no legislation at all to address this form of abuse, while others, such as Canada and France, have introduced specific legislation to criminalise some forms of IBA. In other countries, such as India, elements of IBA are criminalised under existing laws on voyeurism, **privacy**, and information technology. In many contexts, such as in Bangladesh, pornography in general is banned, bringing IBA under the ambit of those laws. This can potentially result in negative repercussions for survivors who consensually share images that the state deems 'pornographic.' In some countries, IBA is also a civil offence, for example under the tort of **privacy** or civil defamation, and victims may be entitled to compensation or damages for the harms suffered.

Many countries, including Bangladesh and India, criminalise IBA as obscenity, pornography, or 'insulting the modesty' of a woman, focusing more on the so-called moral codes rather than the rights of people. Such laws can possibly strip people of their **agency**, and ignore the fact that people may choose to consensually send an intimate image to their partner without wanting it to be shared more widely. Such laws further restrict survivors' **agency** by often preventing them from reporting IBA at all. If they do choose to report it, survivors can find themselves being blamed (or even criminalised) for sharing an image in the first place.

In many countries, laws have limited definitions for intimate images which fail to capture the diverse perceptions of intimacy. For example, India's Information Technology Act 2000 defines a private area as "the naked or undergarment clad genitals, pubic area, buttocks, or female breast." This definition fails to address a host of situations, such as individuals engaged in sexual acts while clothed, or in a state of undress. Importantly, 'intimate' may mean different things to different people. In some communities, covering one's hair signals sexual modesty. If such nuances are not adequately understood and captured within the law, it leaves the door open to a whole range of abuse.

In some countries, including many states in the USA and the UK, the law requires a specific proof of motivation - that there was intent to cause distress. This puts an undue burden on the prosecution because it is often very difficult to prove that somebody intended to cause distress. In fact, in one case, a perpetrator's confession of leaking intimate images of his ex-girlfriend may have actually protected him since he explained his motivation was not to cause distress. Most other sexual offences do not require a malicious motivation to be considered illegal.

Beyond the law itself, lack of adequate implementation delays justice as well. In many countries, police officers indulge in widespread victim blaming when it comes to IBA. Often, law enforcement authorities lack sufficient training and therefore can be callous towards survivors. This is especially true for certain marginalised survivors,

such as sex workers and LGBTQ+ individuals. Moreover, when faced with such barriers at the initial stages of reporting, survivors can often lose **hope** and take no further action towards seeking justice at all. It is concerning to see such a lack of accountability at the implementation level.

In addition to this, processes to seek justice are often focused on efficiency rather than the safety of a survivor. For instance, very few countries allow for anonymity when reporting IBA, and if they do, there are caveats on how much action will be taken. Little effort is made to protect the safety and privacy of the survivor at all levels, whether during trial in court, or while making complaints to the police. There are many ways in which survivors can be involved in the process without having to reveal their identity publicly, such as screening the witness representing the accused, giving evidence by a live link or in private, and putting reporting restrictions in place so their name cannot be used publicly. These are rarely explored, with resource and monetary restraints often cited as an excuse.

Our principles in practice

Despite the many gaps in the law, research also highlights some good practices that show a move towards a more nuanced understanding of IBA and its impacts on victims. In the UK, there are guidelines on prosecuting cases involving communications sent via social media. These guidelines provide a range of information to prosecutors which, if followed, could bring more **accountability** into the process. For example, the guidelines provide further context on tech abuse and its gendered nature, as well as reiterate the role of victim personal statements and community impact statements in describing the wider impact of the abuse. Being able to share their stories could be a powerful way for survivors to reclaim **agency**.

Australia's Enhancing Online Safety Act 2018 addresses **plurality** by expanding the definition of intimate images to include images which depict people without the religious or cultural attire that they consistently wear in public.

South Korea has also been upheld as a good example by providing a comprehensive approach to victim support and redress via its Advocacy Centre for Online Sexual Abuse, which is funded by the Ministry for Gender Equality. In particular, its 26-person-strong team has been praised for putting the survivors' needs and **safety** at the centre of their approach.

Lastly, in Japan, even if no sexual images are distributed, people can consult the police when there is a concern that a perpetrator has intimate images, to seek a way to prevent further damage. This proactive approach can go a long way in safeguarding people from IBA.

Case Study:

Reforming Policy on Cyberflashing

Across the world, only a few countries have laws that expressly criminalise cyberflashing. While Singapore, Scotland, and the state of Texas in the US do have specific laws addressing cyberflashing as a crime, other countries, like India, only allow prosecution of such cases under its more general laws. Without a specific law on the issue, the lack of legal clarity leaves it open for perpetrators to harass people without fear of consequence or **accountability**. Such acts not only threaten a victim's sense of security but are also a serious violation of their bodily autonomy and right to **privacy**. Despite its rise and seriousness, cyberflashing is often trivialised, as the act of sending obscene pictures is considered less harmful than other acts of sexual violence.

> *"Like real-life flashing, cyberflashing can frighten, humiliate, and violate boundaries. It is a form of sexual harassment for which even the physical boundaries of a home offer no respite. [It is] relentless and can cause many women to police their online activity. Yet the trauma is trivialised."* - Wera Hobhouse, Member of Parliament in the UK

When there is no statutory provision that names cyberflashing as a separate crime, law enforcement often ends up trying to fit cases of cyberflashing under other existing legislation, which can mean that the nuances of this crime are missed. For example, currently, in India, cyberflashing can be tried under existing general law provisions which punishes any person who, through words, gestures or sounds, intends to insult the modesty of a woman (section 509 of Indian Penal Code). Alternately, a person can also be tried for publishing or transmitting obscene material in electronic form (section 67 of the Information Technology Act) or for publishing or transmitting sexually explicit conduct in electronic form (section 67 A of the Information Technology Act). Both section 509 of Indian Penal Code and section 67 of Information Technology Act are based on the dated logics of obscenity and modesty which are rooted in paternalism and sexism. Neither is survivor-centred in application, and both acts are vaguely worded: they do not define the scope and meaning of 'modesty of a woman' and 'sexually explicit act', leaving them open to interpretation by law enforcement and judicial bodies. Thus far, only a few cases of cyberflashing have been reported by the media in India and we do not know of any that have been tried under these provisions.

In England and Wales, cyberflashing is set to become illegal in the new (forthcoming 2022) Online Safety Bill. Prior to this, there were a myriad of other laws that could be used but none were sufficient or holistic. Although the Sexual Offences Act criminalises 'exposure', it is restricted to exposure/flashing that occurs in real-time rather than anything recorded in the form of images or videos. Other public order and decency laws theoretically allow for criminalisation of cyberflashing but are primarily based on the condition that more than one person should have been physically present during the occurrence and witnessed the incident. Such laws are not so useful for individual victims who experience such harassment in private, which is common

with cyberflashing. Harassment laws are also restrictive as they require conduct which is oppressive and unacceptable enough to be considered harassment. It is unclear if sending one image would meet this requirement. Further, these laws do not address the sexual nature of the crime, thereby disallowing victims the right to remain anonymous and other related protections guaranteed to victims of sexual assault. The newly proposed Online Harms Bill tries to address these gaps and is a move in the right direction. However, the bill has also been criticised for including 'the motivation requirement' - a requirement that cyberflashing will only be a crime if the perpetrator's motivation and intention was to cause distress, alarm, or humiliation, or to just generate their own sexual pleasure by sending the pictures. This is difficult to prove in court and places undue burden on the survivor.

> *"If the law requires proof of specific motives of offenders, it means that only some women will be protected, and it will be much more difficult to prosecute."* - Clare McGlynn, Professor of Law, Durham University

Our principles in practice

Despite these gaps, there are some good practices implemented globally. For example, Singapore is one of the few countries to have an express provision for the trial of 'sexual exposure'. The Singapore Penal Code criminalises intentional distribution of images of genitals. The law, however, also has a requirement for proving perpetrator's motive, which includes for the purpose of "sexual gratification or causing the victim humiliation, distress or alarm". However, a noteworthy aspect about this law is that the images can be that of the perpetrator's genitals or that of any other person's genitals, thus expanding the scope of what is covered. In addition, by focusing on 'distribution' and not 'receipt' of images, the law also ensures that it is not essential to prove actually receiving or viewing the images for it to be a crime. This shifts **accountability** to the perpetrator, rather than putting further requirements on the victim.

Additionally, in 2019, Texas became the first state in the USA to introduce a specific law on cyberflashing. Under the Texas Penal Code, "unlawful electronic transmission of sexually explicit virtual material" is criminalised. A notable feature of this section is the inclusion of a wide range of activities, such as virtual images of person(s) engaging in sexual conduct, images of exposed intimate parts, and also, images of "covered genitals of a male person that are in discernibly turgid state". The law here starts to recognise the **plurality** of experiences that survivors may have. The broad scope of the section even allows the possibility of extending the provision to the non-consensual sharing of pornography. Further, the only other requirement is proving the intention to distribute images without the express consent of the recipient, thereby doing away with the burdensome requirement of proving the perpetrator's motives.

Another bill recently passed by the Senate of California - the FLASH Act (Forbid Lewd Activity and Sexual Harassment) - is another example of survivor-centred reforms. The bill criminalises the transmission of unsolicited lewd or sexually explicit material by electronic means knowingly by an individual. The images can relate to a range of sexual activities, including exposed genitals and anus, and can be of any person.

There is no requirement of proving the motive of the perpetrator. Further, the provision states that the victim should not have verbally consented to the transmittal of the images and that consent should have been expressly given in writing. By stressing on consent as a key requirement, the bill honours the victim's right to bodily autonomy and **agency**.

Finally, Scotland is another jurisdiction that has passed a specific law for cyberflashing. It categorises "coercing a person into looking at a sexual image" as a sexual offence under the Sexual Offences (Scotland) Act. The 'sexual image' could be of the perpetrator, or any other person real or imagined, thereby allowing fake and photoshopped images to be included within its purview. The law is applicable to both adult and child victims. Though the law creates the requirement of proving motive of sexual gratification or victim's humilation, distress or alarm, it also gives primacy to the element of victim's consent in viewing the images.

By recognising cyberflashing as an offence of sexual nature, the laws in Singapore, Texas, and Scotland ensure that victims are entitled to anonymity and **privacy**, in-camera proceedings, and other special protections in court. This practice ensures and honours the **safety**, **privacy**, and wellbeing of survivors who come forward to report the crime. California's FLASH Act, in particular, is an excellent example of ensuring respect for a victim's agency and consent by making it mandatory for the perpetrator to prove express written consent by the victim. This example is worthy of being emulated in other jurisdictions.

Clare McGlynn and Kelly Johnson's policy brief on cyberflashing, published in March 2021, specifically outlines these elements as vital for an impactful law on cyberflashing, including the need to:

1. Make it a sexual offence, like in Scotland, in order to recognise the nature and harms, to grant victims anonymity and protections in court, and to permit suitable sentencing options.
2. Focus on non-consent instead of perpetrator motives, like in California.
3. Include all non-consensual penis images, like in Texas, in order to ensure the law will be practicably enforceable.
4. Extend motives beyond direct intention to cause distress, like in Singapore.

"Wording of legislation might seem like a small point but it matters if we want to create laws that stand the test of time, that are useful to those who need them most, and to avoid creating laws that are barely worth the papers they are signed in on." - Sophie Gallagher, journalist

4 Building Better Systems

It's clear that systems are currently failing survivors by facilitating abuse, retraumatising survivors, and lacking effective responses and remedies for the harms that are caused. But this is not inevitable. We can build better systems which put the needs and concerns of survivors first, respond to the multitude of experiences and barriers that marginalised people face, and are designed intentionally to support healing from trauma. Exploring what intersectional, survivor-centred, and trauma-informed approaches look like in tech, research, and policy show how this is possible in practice.

4.1 Transforming technology: designing for healing

We've seen how technology can facilitate abuse. But this is by design, not necessity. We propose a model of design which enables technology to be used as a tool to mitigate harm and support healing for survivors of TGBV.

When designing online tools, we need to approach it as though we are designing a physical space - say, a cafe. What do we want people to think about when they stand on the street, looking at our cafe window? What would it feel like if they stepped inside? Would they want to take a seat and linger, or would they want to quickly grab something they need and leave? Do they feel like they can do both depending on their mood and routine?

Applying an intersectional, trauma-informed, and survivor-centred lens presents us with new questions to consider. To ensure the cafe is inviting and comfortable for a wide variety of people with different needs and life experiences, how might we alter the design? If we know that the cafe will welcome survivors who have experienced trauma, what might we change or add to its design?

Likewise, we can think of large social media platforms like towns or cities made up of different communities, infrastructure, and trends. What does it say about our curation of these spaces that so many people feel comfortable shouting, abusing, and threatening to harm others? This behaviour would be addressed by bystanders, community leaders, and authorities in real life, so why isn't this happening online? How can we reimagine online spaces so they reward community and connection rather than conflict and hate?

These are big questions that scholars, activists and platform designers are grappling with. Ethics of technology is an expansive field and there are an ever-growing number of ethics toolkits such as the Ethics for Designers tools, Ethical Design Guide, Consentful Tech Project(and their Consentful Tech Curriculum), Design Ethically Toolkit and Tarot Cards of Tech, that can ground and guide discussions.

But what does transformative, ethical technology design look like when we focus specifically on gender-based violence?

Systemic problems; systemic solutions

We've seen how the systemic problems of market prioritisation, business models, lack of diversity, and power asymmetries influence the way technology platforms enable tech abuse, as well as fail to respond to it. Orbits is focused on providing practical tools that every researcher, policymaker, and designer can use, and the recommendations in this guide can go a long way in better mitigating and responding to tech abuse. However, we also know that harm will continue unless the root causes are tackled. In parallel to immediate interventions, we advocate for the following systemic solutions to transform the tech ecosystem:

Alternative business and governance models: If technology companies are failing to effectively tackle tech abuse because of how their business models operate, alternative business and governance should be part of the solution. Non-profit models, mutual ownership, stakeholder (rather than solely shareholder) engagement, and democratic governance should all be explored as part of the systemic response to tech abuse. For example, the platform co-op movement advocates for tech platforms which are cooperatively owned and governed.

Open source technology: Open source technology refers to software where the source code is open and available to be viewed, re-used, and adapted by everyone. Open source technology promotes collaboration and shared learning between technology companies, rather than competition. It's also resource efficient, easing the high development costs of technology and duplicating efforts, and enabling those resources to be directed elsewhere. All of Chayn's products and services are open source.

Diverse, inclusive teams and management structures: The lack of diversity within tech companies, especially at the senior level, presents major barriers to addressing tech abuse, and implementing the intersectional, survivor-centred, and trauma-informed approach that is required. To remedy this, we must not only diversify these organisations and decision-making teams, but also transform the organisational cultures, management structures, and HR practices that have dominated until now. It is not enough to give 'a seat at the table' to people from more diverse backgrounds, communities, and identities - we must rebuild the tables and the rooms where decisions are made so they can genuinely hold multiple perspectives and facilitate decisions that reflect them.

Check out Mozilla Foundation, Tactical Tech, Algorithmic Justice League, New Public, and Amnesty Tech to learn more about transforming technology.

Learn more about technology design which centres survivors and other marginalised folk in our favourite technology design books: Design Justice by Sasha Costanza-Chock and Design for Safety by Eva PenzeyMoog. For more on developing tech policy, see Superrr Lab's Feminist Tech Principles.

The Santa Clara Principles provide a framework for transparency and accountability in content moderation. Find out more about best practices for gender-inclusive content moderation, compiled by Trust and Safety professionals from the tech industry, here.

IBM have produced five design principles for technology design which are resistant to coercive control. Catalyst's safeguarding resources are designed to help build safe digital services.

Design principles and applications

1. Safety

Safety by design should be a prerequisite for any product but it becomes critical when designing for an audience that has been denied safety, such as survivivors of TGBV. Often, safety risks are minimised or deprioritised in technology design. Instead, we must embrace risk analysis as a way of ensuring more people can use our products, which will improve future outcomes for all.

Application examples:

★ Testing all technology for abusability by conducting threat modelling at multiple stages of the design lifecycle.

★ N2 Factor Authentication.

★ Safety exit button on websites that take users to a non-conspicuous website in case someone is watching them.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.
- ★ Designing reporting mechanisms that don't involve resharing or further distributions of harmful content.
- ★ Blocking and filtering content and users.
- ★ Offering options to restrict how people can get in touch with users.
- ★ Not showing people someone they may know, as it can make someone's secret profile discoverable.
- ★ Not saving information on the user's end as they might be using a shared device.
- ★ In chat bots, providing safety advice before and during conversation.
- ★ The ability to use alternative names, which can help stop stalkers and abusers from finding and tracking survivors.
- ★ Sharing last known logins, so survivors can spot if an abuser or stalker has managed to get control of their devices or accounts.
- ★ Creating user controls on how images can be downloaded and shared.
- ★ Digital fingerprinting, to assist with removing offending materials from all platforms and flagging accounts that shared the offending materials.
- ★ Offering to provide safe contact details as these may differ from the ones that they use to access platforms.
- ★ Providing clear terms of use that highlight zero tolerance for abuse and clearly identify examples of harmful behaviours prominently.
- ★ Permitting third party reporting.
- ★ Reporting to platforms for offline behaviour of users.
- ★ Adding perpetrator information to a digital offender database maintained by the company or law enforcement (if applicable).
- ★ Providing adequate support and trauma counselling for moderation staff.

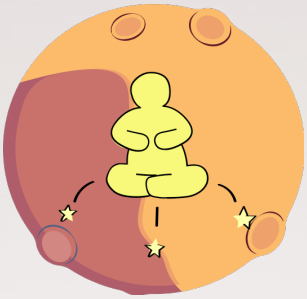
Case Study:

Exit Buttons

Exit buttons are a **safety** feature for websites on sensitive subjects, such as gender-based violence and other forms of abuse. They provide a quick one-click solution to navigate away from the webpage you are viewing, should you need to conceal it from those who are physically nearby. This would be useful in situations where you are in an abusive home, using a public computer, or at work.

As exit buttons have become common practice in recent years, there are some interesting innovations in how to design them. AVA's Breathing Space application lets users choose their own exit page as they are creating an account, and the app remembers their choice. Other websites disguise pages by creating a pop up that covers the website with something innocuous.

For instance, Chayn's exit button 'Leave this site' takes users to Wikipedia's homepage. It used to be Google, but was redirected to Wikipedia to support their mission and because, as the world's number one place to find information, it felt like a good fit. To provide some relief in the moment of panic when someone might need to press the button, not only does the button open a new tab with Wikipedia.com, but also searches 'cute baby animal memes' in the tab where the Chayn website was open. If you click back on the tab, it takes you to a blank screen. In this way, Chayn's button simultaneously deals with physical and emotional **safety**.



2. Agency

Lengthy legal forms that are set out to get consent for data protection are flawed because most users don't want to read through them. Sometimes, it's questioned whether it is safe to expose survivors to co-design processes due to fear of retraumatisation. These attitudes are paternalistic and patronising. We must always centre the user's agency alongside safety, as it is demonstrated that creating environments that value agency can build trust.

Application examples:

★ Offering tools that people can customise and use at their own pace.

★ Refraining from assumptions that survivors of abuse do not want to take an active role in design or feedback.

★ Creating flexible mechanisms that enable people to describe their own experience and share the remedial measures they wish for, rather than forcing reports into rigid, predetermined categories.

★ Allowing people to access essential information without having to create an account.

★ Giving an option of what information is kept public and private, such as full names and location.

★ Building room for consent at various stages, especially in reporting processes. This means 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.

★ Providing comprehensive reporting mechanisms that let survivors report even if the perpetrator deactivates/disconnects their account.

3. Equity

Inclusion by design should be the norm, so that products and services can be used by everyone. When designing products that affect diverse groups, it is crucial to actively be aware of and avoid racial, gender, and class stereotyping, as well as geopolitical differences. For instance, accessibility considerations should support access to people with disabilities, prevent exclusion, and produce a superior, more usable design which promotes a sense of belonging for all.

Application examples:

★ 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.

★ Introducing voice-activated reporting mechanisms to account for different literacy levels and the diverse technology needs of different communities.

★ Rolling out new safety features simultaneously in all low and high-income countries.

★ Making policies and reporting mechanisms available in different languages and dialects.

★ Offering reporting processes with accessibility considerations embedded, including an option for low-bandwidth or offline reporting.

★ Providing staff training and learning opportunities on anti-oppression and decolonisation.

4. Privacy

In an economy where data is considered the currency of interactions, we must consider the harm we may introduce from intrusive data collection, storing, and selling. This involves understanding that some vulnerable groups will not be able to foresee the risks that may arise when they share their data. Data justice acknowledges that information can often be used as a form of oppression by rendering certain communities invisible or misrepresenting them, and thus we need to actively think about how people are counted, represented, and treated through the lens of data science.

Application examples:

★ Securing all databases.

★ Clearly indicating what data is publicly accessible and what isn't.

★ Automatic disabling of cookies and tracking when survivors report abuse on platforms.

★ Only collecting information that is absolutely necessary and creating clear options for more data storage.

★ Using end-to-end encrypted technology.

★ Exploring the use of privacy-enhancing technologies (PET) such as encryption and data masking.

★ Holding entities liable for misuse of sensitive data.

★ Avoiding misleading language and design that can lead to usage of data in ways people have not agreed to (often for profit).

★ Plainly articulating policies in an easily understandable format. If they are long, there should be a summary available so users understand what they are agreeing to.

★ Seeking explicit consent for selling user data where relevant, especially when it is related to marginalised group.

★ Maintaining strict confidentiality for reporting processes.

★ Withholding survivors' details from 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.

Learn more about data justice: Data 4 Black Lives, Te Mana Raraunga (indigenous data sovereignty in New Zealand) and Data Feminism. To benchmark your organisation's data ethics, see the Open Data Institute's Data Ethics Maturity Model.

5. Accountability

When opaque reporting mechanisms, features, and algorithms are commonplace, survivors learn that they should not place their trust in technology. Therefore, technology companies must deliver timely responses and clearly articulate rationales for decisions which impact the safety and lives of survivors.

Application examples:

★ Providing clear ways to help survivors identify in-platform reporting mechanisms. This means quick access bars for reporting abuse, supported by clear wording about what follows.

★ Communicating to survivors which department deals with the report work and informing them that there is a dedicated and specialist resource to handle reports

★ Actioning user research and feedback in design.

★ Sharing openly when something is not working or is a trial feature.

★ Acknowledging gaps in knowledge or foresight which can contribute to harmful features.

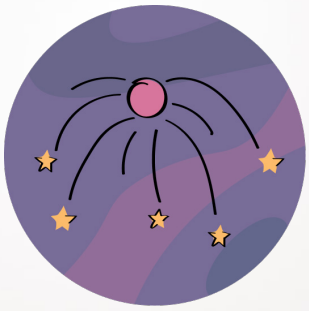
★ Being clear about the hours of your service or the boundaries of your support.

★ Being consistent and predictable in product design - by providing structure and routine, you signal to users that not only have you thought about the service, but are a stable source of support for them. It's not one interaction you're seeking, but the start of a long-term relationship.

★ Committing to long-term change, rather than reacting to scandals and infrequent public outrage.

★ Creating effective and responsive grievance redressal mechanisms on platforms for reporting tech abuse.

★ If applicable, removing the offending user's accounts from other platforms owned by the parent company.



6. Plurality

We need to design for cross-cutting needs, power, and experiences that can change how an individual experiences the digital world and seeks remediation from it. A decolonising design practice will understand the many ways in which harmful stereotypes can turn into assumptions for users.

Application examples:

★ 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 your product or platform.

★ Training staff on the impact of additional vulnerabilities, such as caste, race, religion, sexual orientation, and disabilities.

★ Recognising that people in digital spaces might experience multiple forms of discrimination/hate (for example, gender and race discrimination). Therefore, in complaint processes, it should be possible for survivors to identify multiple offences, including offline ones.

7. Power redistribution

Survivors are often consulted after preventative and restorative measures have been designed. We must ensure that the power to decide those measures lies with the survivor, and that this input is valued through a form of compensation.

Application examples:

★ Giving survivors decision-making power in tech companies through compensated board or committee positions.

★ Consulting communities through different stages of research, design, and implementation.

★ For global firms, using local teams and networks to gather ideas for ways to improve services.

★ Creating community-owned models and practices for governance and evaluation.

★ Translating and localising content and policies.

★ Citing and sharing the work of all feminists and scholars who have influenced or shaped decisions, especially from the Global South.

★ Giving content moderators opportunities to feed into global policies.

8. Hope

In an effort to build rapport with users, some organisations mistakenly use traumatising pictures and words that can be harsh, such as pictures of a man punching down a cowering woman, or a woman crying or covered with bruises. This risks transporting survivors to times when they felt unsafe and, therefore, should be avoided. We should create visual design that uplifts the mood of survivors, and soothes them. Online spaces should feel as warm as possible when someone is feeling unsafe in their physical world.

Application examples:

★ Using an empathetic tone in written and vocal communications.

★ Ensuring visual assets are not retraumatising.

★ Displaying simple, soothing, and visually appealing UX.

★ Prioritising ethical considerations in corporate decision-making over shareholder priorities.

★ Sharing the work of activists, civil society groups, and innovators working to tackle challenges.

★ 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').

★ Thanking survivors for their decision to report through repeated automatic messaging by the individuals who are handling their reports.

★ 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).

Case Study:

Bloom by Chayn - using tech to support healing

Bloom is a remote trauma support service developed by Chayn. In 2020, as COVID-19 lockdowns were introduced around the world, many survivors were trapped at home with their abusers and/or unable to access in-person support systems. Bloom was created as a response to these circumstances, which also filled an existing, serious gap in online, scalable services that survivors anywhere can access for free.

How Bloom works

Bloom delivers trauma support via online courses. Course participants receive access to pre-recorded videos with grounding exercises, information and guidance to support healing, 'homework' activities to do in their own time, and access to 1-2-1 chat with the Bloom team. The courses are designed to be taken over three to eight weeks, but participants can take the course at their own pace. The 1-2-1 chat can be accessed via web browser, WhatsApp or Telegram, and is a space where participants share their reflections and questions on the course content and activities, as well as talk about their experiences of gender-based violence, their recovery journey, or even just how they are feeling.

The aim of Bloom is to 'inform and empower.' To inform, the courses include information on topics such as the fear response and how the body can repeat this response after trauma, and how our sense of self, as well as relationships with others, can be affected by trauma. To empower, it includes practical tools for grounding ourselves in the present, assertive communication techniques for healthy relationships, and a variety of journaling techniques for exploring our own stories and healing. All of this is grounded in an intersectional feminist worldview, that takes a critical look at the ways society enables predators and abusers. Bloom clearly communicates that abuse is never the survivor's fault. The course content is developed and written by survivors in collaboration with a trauma-informed therapist.

In 2021, Bloom ran five courses: Creating Boundaries, Managing Anxiety, Healing from Sexual Trauma, Recovering from Toxic and Abusive Relationships, and Reclaiming Resilience in Your Trauma Story. Bloom also launched an industry-first partnership with dating app Bumble, by providing a customised version of Bloom to Bumble users who report sexual abuse or assault. By the end of 2021, Bloom had supported over 1,000 survivors from over 60 countries. 97% of Bloom users would recommend the programme to someone in their position.

> *"Through Bloom, we see the kind of deep impact that comes from people understanding how trauma has impacted them, and how sexism shapes even the way you deal with it. 40% of survivors who take our course have never been to a therapist due to lack of affordability, stigma, or fear of being seen."* - Hera Hussain, Founder & CEO, Chayn

Our principles in practice

Bloom prioritises **privacy** by making all courses completely anonymous - participants do not have to share their real name or any personal information to take part. Participants do not interact with each other or find out who else is doing the course, but they work alongside other survivors and are continuously reminded through the courses that they are not alone and 'are in this together'. In this way, they benefit from group learning, without compromising on **safety**. The **safety** of Bloom is further supported through safeguarding processes, including mandatory safeguarding training for all Bloom team members.

To ensure the **agency** of survivors, the courses are made to be flexible - participants can learn at their own pace. They can watch the videos and complete the activities whenever it is convenient for them. This adaptability responds to a **plurality** of survivor experiences and needs. Moreover, participants actively shape the course - the course content is continuously adapted and improved by feedback received during the courses and from regular user research interviews. In this way, Bloom practises **power redistribution**, too.

Bloom also promotes **equity** by ensuring the course content is relevant for all survivors, and uses examples which particularly highlight the experiences of marginalised groups. Since the service is completely free, no-one is priced out. To improve accessibility, transcripts are available for all course sessions, in addition to the videos, and all videos have captions which are edited for accuracy.

Hope is central to Bloom - the foundational message of all courses is that healing from trauma is possible for every survivor. Moreover, Bloom seeks to inspire **hope** in each participant through inviting, soothing UX and by starting each video with a grounding exercise. These grounding exercises are designed to help participants mentally distance themselves from their daily lives and physical surroundings, and feel physically and psychologically present in Bloom's online space.

In response to the growing rate of tech abuse, Chayn has started working on a new Bloom course, focused on image-based abuse.

Case Study:

Tech Policy Design Lab - co-creating tech policy solutions to end online GBV

The Tech Policy Design Lab, an initiative of the Web Foundation, aimed to create innovative tech-policy solutions for building a safer and more equitable internet, free from GBV. From March 2020 to February 2021, the Web Foundation hosted a series of four multi-stakeholder consultation workshops to explore and build understanding about online GBV on women activists, women in public life, and young women. The findings from these consultations were used to develop three policy design workshops in April 2021. Partnering with service designers Craig Walker and Feminist Internet, the Web Foundation brought together the world's largest tech platforms, policymakers, academics, and civil society organisations to co-create solutions for tackling online GBV through multi-stakholder workshops. This project especially focused on women in highly public-facing roles (such as politicians, journalists, and activists) leading active online lives. Based on the insights from the consultation workshops, policy design was concentrated on two areas of great importance for creating a safer internet for women: curation and reporting.

Curation: Greater control over who can comment or reply to posts, as well as more choice over what women see online, when they see it, and how they see it.

Reporting: Improved reporting systems so women can be better supported when they do receive violent or abusive content.

Policy design method

The Tech Policy Design Lab used design thinking and co-creation methodologies to generate potential policy solutions around these two themes. Participants worked in small multi-stakeholder groups and were given a specific scenario to design for, including a fictional persona, app, and problem. While the scenarios were hypothetical, they were based on the real, lived experiences of women facing online GBV. The personas were chosen to represent intersecting identities (for example, race, sexuality, and gender identity) to encourage solutions to take an intersectional approach. Using this methodology, participants were able to design solutions based on the needs of survivors, rather than being limited by currently available tech solutions.

"While we can't quickly unwind the sexism that drives abuse, we can redesign our digital spaces and change the online environments that allow this misogyny to thrive." - Azmina Dhrodia, **Safety** Policy Lead, Bumble (formerly Senior Policy Manager, Web Foundation)

Prototypes

The workshops generated 11 promising prototypes for tackling online GBV. For example, Reporteroo is a prototype that affords transparency for users in the reporting process by allowing simple, real-time access to information about follow-ups, and also providing the option of reporting in local languages along with the provision to add context-specific information of the incident. Another prototype, Com Mod, allows users to appoint trusted users who can then moderate comments on the user's behalf. The actions taken by trusted users can be approved or reversed by the original user if needed. This prototype reduces the burden of trauma experienced by women facing abuse by reducing the amount of abuse they see and allowing delegation of removal/blocking/restricting of abusive comments to someone they trust. These collaborative solutions explore the scope for community intervention and prioritise the **safety** of vulnerable users.

Recommendations

The final report on Online Gender-Based Violence and Abuse was released by Tech Policy Design Lab in June 2021. Based on the workshop discussion and prototypes developed, the report includes user-centric recommendations, design suggestions about how recommendations could be achieved, illustrative examples of what the recommendations could look like in practice, and other considerations that should be taken into account when introducing these measures, such as technical challenges, required policy changes, and the possibility of misuse.

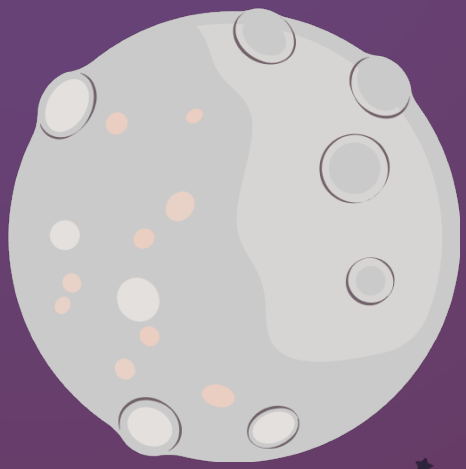
Curation	Reporting
1. Offering more granular settings (e.g. who can see, share, comment, or reply to posts) 2. Using simple and accessible language throughout the user experience 3. Providing easy navigation and access to **safety** tools 4. Reducing the burden on women by proactively reducing the amount of abuse they see	1. Offering users the ability to track and manage their reports 2. Enabling greater capacity to address context and/or language 3. Providing more policy and product guidance when reporting abuse 4. Establishing additional ways for women to access help and support during the reporting process

The Tech Policy Design Lab not only generated concrete suggestions for how to design technology that addresses online GBV, but also demonstrated how survivor-centred, trauma-informed, and intersectional policies can and should be developed. By clearly detailing their process as well as their findings, the Web Foundation offers a blueprint for technology companies on how they can work together with civil society, academia, and survivors to co-create policy and design solutions that effectively tackle GBV on their platforms. The participation of representatives from big tech companies like Facebook, Google, Twitter, and TikTok in the workshops means they now have first-hand experience of this process. The Tech Policy Design Lab acts as a benchmark against which the tech companies' progress can be measured.

Our principles in practice

The Tech Policy Design Lab supported **power redistribution** by creating multi-stakeholder spaces where everyone worked together to create solutions. Moreover, it encouraged **accountability** from the world's most powerful tech platforms by involving them in the process. By adopting a design thinking methodology, and creating personas with intersecting identities, **plurality** and **equity** are prioritised.

Tech Policy Design Lab's recommendations promote **agency** (by focusing on curation of content by survivors, and more oversight and control in the reporting process) and **safety** (by recommending how to restrict the amount of abuse women see online and offer more support throughout the reporting process). By initiating this project, sharing their process and insights openly, and making concrete recommendations to tech platforms, they offer **hope** for a better, safer, and more inclusive internet.



Case Study:

Pex - fighting IBA with technology

Pex is a digital rights technology company enabling the fair and transparent use of copyrighted content on the internet. Founded in 2014, Pex has developed a copyright solution for the creator economy known as Attribution Engine, which enables content identification on digital platforms so that creators and rightsholders can be acknowledged and credited for their work. When building their Attribution Engine, the Pex team recognised that it could be used for another purpose too: helping to prevent the spread of toxic content, including image-based abuse.

> *"Technology alone isn't going to solve the problem, but it needs to be a massive part of the solution. The internet is still the wild west and we have so much opportunity to make it a better place for everyone."* - Chanelle Murphy, Product Manager of Trust and **Safety** Division, Pex

Pex's Trust and **Safety** division has developed a feature designed specifically for preventing the publication of known toxic content on platforms. Built with Pex's leading fingerprinting technology, Attribution Engine can scan videos and images for known abusive content and send information about the content automatically to the appropriate digital platforms so that it can be flagged for removal or blocked before it gets published. Pex partners with trusted non-profit organisations who are provided a user-friendly software development kit that creates fingerprints locally. The fingerprint is then sent to Pex and compared against user-generated content, or UGC, fingerprints in real time. If a match is identified, the content-sharing platform is notified and Image-Based Abuse (IBA) is blocked from the platform before it is ever posted. These results are communicated back to a Pex dashboard, which shows non-profits where the content has been uploaded or blocked. Pex does not store the content in its original form, and digital fingerprints cannot be re-programmed to derive original images.

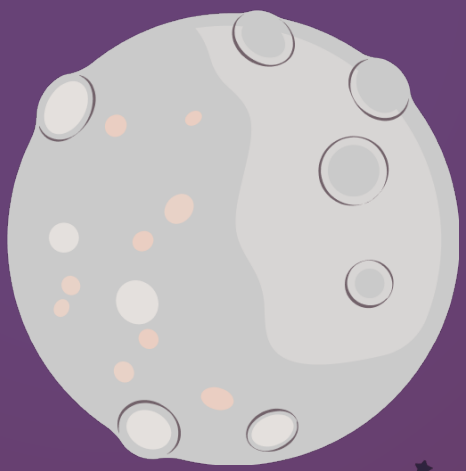
Alongside creating this tech, Pex has also begun community engagement work on the issue of IBA. Since IBA is a reflection of societal attitudes and prejudices, Pex sees a role for facilitating conversations to raise awareness about this topic, build solidarity and empathy for survivors, and shift the narrative. For this, Pex has started an initiative called the Trust and Safety Internal Community, in which Pex staff meet to talk and learn about different kinds of IBA, its prevalence, and the implications on survivors' lives. They **hope** these discussions will motivate employees to speak to their families and friends, and to become advocates against IBA in their communities.

> *"This is a fundamental-societal problem, and it's going to take a lot of voices coming together, in addition to heavy tech solutions."* - Chanelle Murphy

Our principles in practice

The capabilities of Pex's technology improve **privacy** and **safety** for survivors, by providing an effective route to report and remove IBA, without needing to continuously share or engage with it. Pex prioritises the emotional **safety** of survivors too, by collaborating with trusted non-profits to deliver this tool so that survivors know they can trust the process. Simple design with step-by-step guidance on reporting abuse makes removal of IBA content easier for the non-profit staff, reducing the risk of vicarious trauma.

Pex's Trust and **Safety** team have worked extensively with survivor advocates and non-profits to develop the technology, showing a commitment to **power redistribution**. By enabling non-profits to report their IBA content and have it not only removed but also blocked from future uploads, Pex provides a beacon of **hope** for survivors.



Case Study:

Digital Rights Foundation - Cyber Harassment Helpline

Digital Rights Foundation (DRF) is a feminist, not-for-profit organisation based in Pakistan. Founded in 2013 by lawyer Nighat Dad, DRF defends digital freedoms and rights through awareness-raising, research, and policy advocacy. One of their priority aims is protecting women and other marginalised groups from online harassment.

In 2016, after running an awareness campaign about online harassment and digital safety, the DRF team found themselves inundated with messages from women looking for guidance and help with cases of cyber harassment. DRF recognised the need for a dedicated channel to deal with these enquiries and later that year, established the Cyber Harassment Helpline - the region's first helpline for these kinds of cases. Today, the helpline receives an average of 212 calls per month.

> *"And we have seen that the number of such complaints never decreases at the helpline. It always increases. Even though there is a lot of awareness. Despite the fact that we have a "cyber crime law" that aims to protect women online."*- Nighat Dad, Executive Director, Digital Rights Foundation

The helpline receives calls on many different types of online violence, including hacking, online stalking, doxxing, impersonation, and abusive language. However, their most common cause of complaint (around a third of overall calls to the helpline) relates to blackmailing: when threats and demands are made based on sharing an individual's personal information and/or photos without their consent. This presents particular dangers in Pakistan, where cultural and religious norms mean information and photos shared online can be the cause of great shame and backlash. This can therefore restrict a survivor's ability to exist online, as well as have serious offline risks for survivors including mental health implications, punishment from family, restriction of other freedoms (for example, the opportunity to go to university or work), and violence.

While the helpline was originally set up to provide digital security support, the service has now expanded to offer psychological counselling and legal assistance to keep up with the demand. Over a quarter of callers require legal assistance, and DRF has a network of lawyers who offer pro bono legal support to callers. Helpline support staff are all trained in psychological support and can assess distressed callers against mental health indicators, referring them to DRF's in-house psychologist if they are found to be at risk.

Our principles in practice

Privacy is foundational to how the helpline operates. DRF prioritises caller confidentiality and does not collect any information which is personally identifiable. If it's assessed that the call might be cut off, phone numbers are temporarily stored so DRF can contact the caller, but numbers are never collected in permanent records. Prioritising the **agency** of survivors, the DRF team is very careful about if and when they use survivor stories in their advocacy or awareness-raising work. When they do, they work with survivors whose case has been resolved or come to some sort of conclusion, and/or those they have a long-standing relationship with. They are also careful to inform survivors about exactly how and why the information will be used, ensure they are providing remedial resources throughout the process, and protect the survivors' anonymity.

Learn more about Nighat Dad's work and life story in this Digital Rights & Feminist Future zine.

4.2 Rethinking research: enrichment not extraction

It is possible for researchers to design settings and processes that are non-extractive, affirming, and enabling. Many survivors are eager to participate in research because they have experiences of not being heard or believed, and because they want to share their own experience to help others going through the same trauma. Trauma survivors report benefits from engaging in research including feelings of validation, catharsis, or altruism. Understanding this and putting survivors and their many different experiences, perspectives, and needs at the centre of your research process is imperative. Research on trauma does not need to be extractive or retraumatising; it can be enriching.

Design Beku, a design agency in India, introduced the distinction between extractive and enriching experiences when talking about their research into pregnancy care in rural India:

"The foundation of any ethical research framework is the approach, which must choose to be enriching rather than extractive from the outset. This means discarding stereotypes of researcher-respondent relationships and creating a collaborative system where everyone is a co-creator. This requires thinking through ways in which one can consider, engage, and determine with user communities what should be researched, how that research should be conducted, and how the data should be shared."

For leading academic research on TGBV, check out University College London SteAPP and Queensland University of Technology.

Women's Aid Research Integrity Framework provides a framework to consider and discuss what feminist, ethical research of GBV looks like.

Participatory methods

Participatory methods have shifted traditional research dynamics of the passive 'subject' and 'expert' researcher. They have opened up exciting opportunities to challenge how agency, power, and consent are practised. However, no research method should be viewed as a silver bullet.

Jagosh et. al describe participatory research as a discipline that prioritises "co-constructing research through partnerships between researchers and stakeholders, community members, or others with insider knowledge and lived expertise."

Usually, participatory research will involve stages of planning, recruitment, collaborative research techniques, data collection, analysis, and plans for iteration. Not all participatory methods are appropriate or needed, and when they are, they require care and active facilitation. There must be degrees of participation from people with

lived experiences and these must be calibrated on a case-by-case basis. Just because a research is participatory doesn't mean that it cannot be harmful in itself - all other ethical considerations remain just as important.

Participatory research can take many forms. In the technology space, user-centred design is most commonly used and therefore will be our focus. In this field, most user-centred design research is done with primary interviews with survivors of gender-based violence, as well as a mix of traditional methods such as surveys and focus groups.

With some groups, a qualitative approach might be better suited; this can include receiving interview responses via a series of voice notes on a messaging app, asking a question in a social media group where there is already established trust, or just observing natural behaviour during an activity. These techniques can add more context and fill the gaps present in a purely quantitative approach.

For participatory research, feedback loops must be active and adaptive. Survivors should be involved in as many stages as appropriate and must be informed of the progress of the project. Within Chayn and End Cyber Abuse, for example, participatory research is done with survivors who form part of the team and have decision-making power, and also involves survivors from outside of our teams so that we always consider more perspectives. Survivors should not be seen as informants who simply provide data points.

At the same time, we must acknowledge that research into gender-based violence is trauma-inducing, and is difficult for not just the survivor but also the researcher.

Steps taken to create an enriching environment for survivors will also benefit the researcher, and wellbeing measures for the research team should also form part of the project design. Organisations should include survivors in long-term decision-making where technology and research design will have a direct impact on how platforms can become a tool for violence. However, even in research projects based on short-term models and deductive methods - as is common in the technology sector - we can apply the Orbits design principles to ensure the process is intersectional, trauma-informed, and survivor-centred.

Research process

We advocate for research projects that are participatory and involve the following layers (though not always). These layers will not necessarily take place in this order. These are based on our experience of undertaking research within a user centred product design process, alongside the input of stakeholders who undertake wide ranging research approaches and methodologies in diverse settings. These layers follow good practice in research design, but are often overlooked in the context of tight timeframes and limited budgets, particularly in technology design settings.

★ **Reflection and ethical exploration:** Before embarking on a research project, the first question to ask is why? You should start with considering why the research is important and exploring the ethical implications and questions that might arise. For example, in Django Paris and Maisha T. Winn's book Humanizing Research: Decolonizing Qualitative Inquiry with Youth and Communities, the following

questions are helpful:

1. *Why are you engaging in this research project? Who will it impact? How and why?*
2. *Who will you collaborate with to engage in this research? How will these relationships be established? What are your political goals for this research project? What contributions can you make toward these political goals in addition to your research?*
3. *How have your emotions shaped how and what you research? What emotions are produced through your research? How are these emotions linked to wider circulations of public feeling? How have your emotions shifted throughout the research process?*
4. *After the research is completed, what are your ongoing commitments to the political goals you identified as important for this research?*

Engaging in this sort of reflection upfront will help to refine the research plan, unearth any key ethical considerations, and ground the rest of the process with clear purpose and intention.

★ **Hypothesis:** What are we trying to find out? What do we know? What's unknown?

A clear purpose and mapping of assumptions sets the project up for success. This might involve an in-depth discussion with your team and could also involve the Consequences Scanning exercise by Doteveryone, a process which unearths the possible positive and negative consequences, intended and unintended, of your research and technological intervention.

★ **Desk research:** What can we find out from existing research that can help us refine our hypothesis?

Using your own research archives and those of others in the public domain, you can cut down on the amount of trauma extraction, inefficient research design, and time spent on re-doing a piece of work that has been done many times before. For example, we already know survivors of tech abuse are often not taken as seriously as those that experience physical assault. It's been shown in many high-profile cases, studies, and surveys. This is not to say that this question cannot be asked if it makes sense for the context, but we can form better questions having known the history.

★ **Internal group research:** What knowledge do we already hold in-house?

There's a wealth of knowledge within our team members, especially if they come from a diverse set of life experiences and backgrounds. We should use it.

Test ideas and do research sprints within the team before going outside. This enables us to test our questions and approach, and also gather valuable data from people who are already invested in and have co-designed the process. It's important to understand where the gaps in knowledge and experiences are likely to be, as no team can be perfectly diverse or capture all perspectives that are important for your project.

★ **External research:** Who can we speak to, learn from, and collaborate with to build on and test our hypothesis?

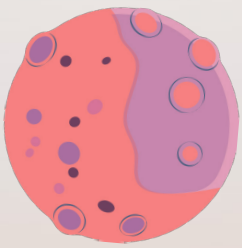
By this point, we usually have a more refined research plan and can embark on finding interviewees and participants. This is when we focus on questions of remuneration, safety, and creating a warm space online or offline. The hardest part is going beyond a known community that we already have access to because unless your project is hyperlocal, doing different research with the same people is likely going to result in significant gaps. It's vital that we ensure participants have the agency to refuse participation altogether or are involved in varying degrees based on their preferences.

★ **Internal synthesis:** How can we make sense of what we've heard? What conclusions can we draw from it?

The synthesis requires us to explore and identify common themes emerging from the data, look at enablers, barriers, and needs, and make a plan for research gaps. This can form a first draft of insights.

★ **Open findings:** How can we share our analysis to improve and enrich it?

This gives participants a chance to see what the conclusions and insights have been gathered, so that they can comment to correct mistakes, if any, and also build on what's been documented. You can also open this draft to other organisations in your sector and/or share publicly but care must be taken to provide sufficient context and anonymise any survivor input. Inviting comments and feedback on an open research is inherently enriching, and not extractive, as it contributes to open knowledge rather than accumulating information for just one organisation's benefit.



★ **Recalibration:** How can we incorporate ideas and feedback into a coherent analysis?

This requires us to validate what is known and identify what's still missing. We repeat the synthesis process from before but with more scrutiny because advice, feedback, and edits have come from people who do not know enough about the particular issue. This is one of the dangers of open feedback, so rather than looking at the number of responses, we have to capture the merit of each one and assess how relatable it is for our work.

★ **Use and re-use:** How can we best use what we have and share it with others so it enriches their work too?

Research analysis must inform product and policy design, otherwise it does a great disservice to all involved, especially survivors who share their trauma to improve things for others. Research projects do not end when the research is complete; rather it is our responsibility to disseminate and stimulate uptake of the research findings. This should be considered and encouraged throughout the research process, and should not be an afterthought.

We must explore ways to make such research re-usable by others. Writing reports and blogs is useful here, but there's more that can be done.

One exciting idea is to create an open research library for the entire ecosystem to reduce the need for re-doing research, as design agency Snook have done with the local council in Hackney, London. This would include things like user needs, statements, quotes, and anecdotes that can be categorised and tagged for ease of finding. Opening up research in this way would also enable us to focus our collective efforts on identifying and filling gaps.

★ **Storytelling:** What is the most impactful way we can recount what we've researched?

In many cases, storytelling is an instrumental part of using research for change. Simply presenting research is not always sufficient to really communicate the full weight of the findings. Especially in the case of GBV, storytelling helps to illustrate the depth and nuance of the pain, trauma, resilience of survivors, and the complexities of each story.

"It is important to combine qualitative data with survivor stories to make people see what it's really like."

Mariana G. Valente, Director

"At Luchadoras, research and healing go hand in hand. Most research sessions are participatory and also informative. Instead of approaching the research with a theory or hypothesis first, Luchadoras, first spends time simply listening and documenting the lived experiences of the participants. Only once they have a good grasp of this, do they aim to connect these experiences with an existing theory on the field."

Lulu V. Barrerra, Luchadoras

Design principles and applications

The Orbits principles can be used to demonstrate what enriching research looks like, and to avoid using extractive practices. Though we focus on gender-based violence, these principles can be applied to any research setting with a vulnerable group.

1. Safety

Ensuring that survivors' safety is not threatened by their participation is research is paramount, and taking care of their emotional safety is equally important. We must design research settings where survivors feel safe, secure, and able to participate fully.

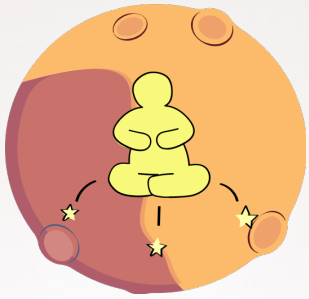
Application examples:

- ★ Carefully considering who to involve in the research - just because someone is up for the research doesn't mean it is the best thing for them.
- ★ Clearly communicating to participants about what topics will be covered.
- ★ Offering interviewees the option of choosing the time and channel of communication.
- ★ Building a relationship with participants through pre-research checks.
- ★ Building a rapport at the beginning of interviews.
- ★ Being mindful of interviewees' body language and take a break if you think they might need it.
- ★ Offering a debrief with researchers and/or a restorative activity like mindfulness, yoga, or a walk.

★ Offering interviewees the option of choosing the time and channel of communication.

★ Offering a therapist right after sessions or as support that they can use later on. Prompt this in follow-ups.

★ Establishing referral pathways to services.



2. Agency

Survivors can feel a great sense of agency just by participating in research,but we must also be mindful to design the research process in such a manner that this agency is respected and maintained.

Application examples:

★ Seeking informed consent. We must ensure participants understand and fully consent to the ways their stories and contributions will be stored, shared, and attributed to them.

★ Offering multiple ways to opt out of research.

★ Giving generous time scales at every stage of the research (giving initial consent, approving final product) to allow participants space to read and digest information.

★ Offering different options for contributing to research (for example: audio, video, submitting a piece of writing, or reviewing what you've written).

★ Not restricting survivor's input to only interviews if they want to be involved in other ways. If they've offered to do more because they want to, that's not an extractive practice. This can come from a place of empowerment.

★ Acknowledging and affirming the contributions of survivors.

3. Equity

An equitable approach to research means that we must acknowledge how different forms of oppression might restrict or impact someone's way of engaging, and create research settings that mitigate this risk. Where barriers to participation exist, extra support should be provided.

Application examples:

- ★ Compensating people. Keeping in mind that there may be legal restrictions for some to accept money, provide alternatives like vouchers for food.
- ★ Providing nursery and child-caring responsibilities, as well as helping with travel costs.
- ★ Letting people talk about challenges that go beyond your subject arealf someone struggles to name their experience, ask them how it felt instead. And once they have explained, validate their experience and name it so they can take that awareness with them.
- ★ Physical and online spaces need to be accessible to people with disabilities.

4. Privacy

A survivor's choice to contribute towards research should never impact their privacy. Strict confidentiality policies and processes are prerequisites, and they should be followed at all times.

Application examples:

★ Deleting voice and video recordings after a certain period of time. You can keep an anonymised script.

★ Making survivor testimonies anonymous by default. Allow people to choose their own pseudonym. Remember that some people want to share their stories with their names as part of their healing journey so if your project has space to give that visibility, do that.

★ If conducting research for a company that the survivor is a user of, offering survivors the option to have their views decoupled from their user account.

5. Accountability

Researchers should be open about the details, scope, and limitations of their research, and establish two-way communication and feedback loops with participants.

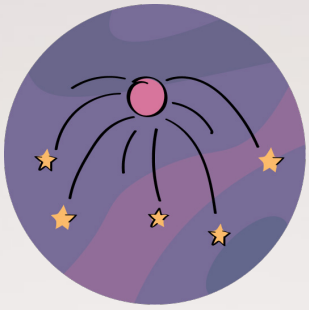
Application examples:

★ Being transparent about the process, time, and compensation from the outset.

★ Being upfront about gaps in knowledge and how systemic bias may affect the project.

★ Responding to questions in a thorough and timely manner.

★ Being clear about sample sizes. Small sample sizes, even when diverse, can give misleading results if they are used to represent their entire community or a larger, diverse population.



6. Plurality

The purpose of doing research is to understand different survivor experiences - and they will be different. Our research design should create space for that and strive to capture the complexity and diversity of different views and perspectives.

Application examples:

★ Mitigating the impact of group participation where some participant(s) are uncomfortable or alienated due to their identity or cultural background.Mitigating the impact of group participation where some participant(s) are uncomfortable or alienated due to their identity or cultural background. Avoiding leading questions.

★ Leaving space for interviewees to share what they want to share about other aspects of their life that are relevant to them.

★ Letting the interviewee lead the conversation.

★ Considering and capturing the context of the experience.

7. Power redistribution

Researchers may not feel powerful in the context of the technology and policy ecosystem they are researching, but within the confines of the research environment, they hold an incredible amount of power. All efforts should be made to share this power with participants as well and enable them to harness it through the research process.

Application examples:

★ Giving survivors decision-making roles in research projects.

★ Working with survivors to shape the research (e.g. in defining the scope of the research or co-creating research questions)

★ Letting interviewees choose aspects of the interview (e.g who the interviewer will be, what's the interview medium)

★ Giving interviewees review and final sign off over anything produced with their story.

★ Creating space for interviewees to co-design and provide feedback on the research process.

8. Hope

There are many ways that research can offer hope to survivors: by demonstrating that they are heard and believed, creating a space of solace, and contributing towards systemic changes. Regardless of the aims and outcomes of the research, the design should inspire hope for the participants.

Application examples:

★ Creating warm interview and research spaces, online and offline. Comfortable, non-clinical ambience, especially for those who have experienced oppression at the hands of police and/or state, is likely to result in more open and explorative conversations. Recreating this online can be much harder, but is possible through friendly facial expressions and grounding exercises.

★ Always leaving space for reflection at the end of an interview. Not ending conversations abruptly. Where possible, end the interview on a positive note.

★ Planning how you will use the research to actively affect change and sharing with participants how their story is going to improve conditions for others.

★ Thanking survivors for their contributions to any research projects.

Case Study:

InternetLab - researching TGBV for impact

InternetLab is an independent Brazilian research centre working on issues related to law, technology, and the internet. Their work focuses on five thematic areas: privacy and surveillance, freedom of expression, information and politics, inequalities and identities, and culture and knowledge. As part of several of these streams, especially inequalities and identities, they have done extensive work on gender, including TGBV, and have demonstrated ways in which non-extractive research can form part of effective interventions to tackle tech abuse.

Research methods

For InternetLab, one of the most important aspects of doing trauma-informed research is understanding when it isn't appropriate or necessary to do the research at all, or when you are not the right researcher or research organisation to be undertaking it. For example, since 2015, the organisation has researched non-consensual intimate images (NCII) in Brazil and beyond. As part of this work, a case study was done in certain schools in the city of São Paulo, where NCII was happening to teenage girls at an alarming rate and, tragically, had resulted in several suicides. Given the sensitivity of the subject matter and how young the affected women were, the InternetLab team realised that they did not have the required experience to carry out research with the survivors responsibly. Instead, they spoke to local activists who were working closely with the survivors on this issue. In this way, they were able to ensure the voices of survivors were central to their research, without taking the risk of retraumatising them.

> *"I don't think it's a problem to speak to survivors at all, but I think you have to consider case by case if you have the correct skills in your team and if the situation allows. I think there's gonna be situations in which these people just need to be protected from speaking, but it's very different to situations when survivors want to go out and reach the world with their stories and they are ready for that. I think having the skills in your own team to be able to differentiate those situations is really important."*
>
> Mariana Valente, Director, InternetLab

InternetLab continuously experiments with different ways to practice trauma-informed, non-extractive research. For example, in 2017 they applied action research methodology on a research project which was about domestic workers in São Paolo and their use of technology. The project worked with a group of 30 domestic workers to develop the questions and analyse the results. Having domestic workers interpret the research themselves yielded much more in-depth and accurate results. For example, the research found that only 8% of domestic workers said that the internet was helping them find work. While the researchers might have assumed that this

implied that domestic workers did not know how to use the internet to effectively find work, the workers explained that it was not an issue of ability but safety. Because of multiple experiences of violence or harassment when doing domestic work, they do not want to work for people they don't know, and thus prefer to get work through their own networks rather than going online. Employing this action research methodology therefore enabled InternetLab to get richer insights.

Influencing policy and the media

> *"I really believe that research is really important, but have also learnt that just doing research reports - that are so difficult to read and are so long that we just put out in the world and expect people to read - is probably not going to make the full difference that we want it to. Of course it's not that it's not relevant at all, and some people might pick it up and make it more simple and make it more straightforward, but it's really important to think of these strategies of calling attention to the things you're doing."*
>
> Mariana Valente

The InternetLab team also innovates with ways to make sure their research has an impact - in the media, and on policy. For example, as part of their work on NCII, they partnered with the University of São Paulo to influence the legislative process around a bill that was being developed in response to NCII. They worked with a group of law students and, together, went to the capital of Brazil to deliver the policy paper to the rapporteur working on the bill. The students explained the issues identified in the research and why their recommendations were so important. The rapporteur listened and their recommendations were implemented. Partnering with a well-respected educational institution, and having students lead the engagement with policy makers, was instrumental in getting this successful result.

Another example comes from the 2020 municipal elections in Brazil. InternetLab partnered with feminist news organisation Azmina to monitor and research online hate and harrassment targetting female candidates. During the run-up to the election, they worked with Azmina to not only research the harassment as it was unfolding but also, crucially, to disseminate their research through the media. The impact of this was huge: candidates mentioned the research during the election and, in some cases, used it to speak out about the abuse they were facing. By directing attention towards their research, InternetLab was able to highlight the extent of the issue and advance conversation about the necessity for policy to address it.

Our principles in practice

InternetLab prioritises **safety** by considering carefully when it is appropriate to do research directly with survivors, and whether or not they have the necessary expertise to carry out the research. They also employ the principles of **agency** and **power redistribution**, by finding ways for research subjects to actively shape the research design and contribute to the research analysis. Finally, by not only carrying out the research but continuously finding partnerships that will help the research have an impact in the real world, the InternetLab demonstrates and exemplifies the principle of **hope** - and shows how research can be an effective tool to tackle tech abuse.

Case Study:

Point of View: Storytelling for change

Point of View is a non-profit organisation based in Mumbai, India which works towards building and amplifying the voices of women and other marginalised genders. They are a collective of gender rights activists and researchers, with vast experience working with women, LGBTQ+ persons, and people with disabilities, especially those belonging to low-income groups. Their work has been instrumental in breaking stereotypes and changing the narrative on sex, desire, and gender roles in India. Point of View centres their work on issues at the intersection of gender, sexuality, and digital technologies and is involved in research, advocacy and spreading rights awareness. Since 2017, Point of View has been conducting digital literacy, skills, and resilience building workshops with marginalised women, girls, and queer persons from grassroots communities across India. The workshops help enhance the understanding of tech abuse, harassment, and violence, how to deal with these in different ways, and reduce TGBV.

Storytelling

Point of View uses storytelling as a tool to tackle tech abuse. They document and disseminate stories through several zines, shift the narrative on gender, and advocate for societal change. In 2019, they published 'Free to be Mobile', a zine documenting ten stories of everyday struggles and resistance against digital violence. They published anonymised accounts of women, girls, and queer and trans-persons across India who experienced violence perpetrated through mobile phones, including those that are not connected to the Internet. In doing so, they highlighted how violence carried out through telecommunications is often ignored in conversations about tech abuse, which often focuses on social media. The research demonstrated the prevalence of "wrong number" harassment, location tracking, WhatsApp hacking, and checking of itemised phone bills by male family members, among other kinds of digital violence through phones, and how each story was rooted in questions of gender and access. Through their storytelling, they were able to show the diversity of tech abuse and survivor experiences. The zine powerfully portrayed how survivors are leading resistance against tech abuse, as it shared stories of home-spun remedies to counter violence, comforting and supporting others facing similar issues, and creating space for solidarity and empathy.

> *"Stories really give survivors a sort of credibility. They honour the experience... storytelling is incredibly powerful and I think it's actually an overlooked tool when we think about dealing with GBV. It makes cases real, considering digital violence is always put at a lower pedestal."*
>
> Bishakha Datta, Executive Director, Point of View

Prioritising lived experience

Lived experiences are central to their approach. Point of View operates on the philosophy that 'survivors know best' and hence, sources research and solutions from the lived experiences of survivors. They centre survivor's consent at every step in the creation, delivery, and sharing of stories to ensure survivors retain control over how their stories are told.

> *"Survivors know it best. That's the simple reason why survivors should lead these kinds of initiatives. We really believe quite strongly at Point of View that lived experience is at the heart of good policy making, good advocacy, good responses to GBV."*
>
> Bishakha Datta

Giving primacy to lived experience shapes and deepens Point of View's analysis of tech abuse, and generates new ideas for solutions. For example, their work with sex workers has highlighted the importance of multi-modal, not text-based communication. Most of the sex workers they work with cannot read or write, but do use mobile phones for personal and private matters. Given they cannot write, when they save somebody's number they use emojis: someone is a lion, somebody else is a tiger, another person is a rose. Point of View therefore highlights the importance of building non-written communication into tech platform design, such as visible buttons and symbols, and using voice for reporting processes.

The consideration of lived experiences shapes the way Point of View delivers their community workshops too. They operate a peer training model, where they train a number of people to train and share their learnings with a larger group in their community. For example, during the COVID-19 pandemic, Point of View trained domestic workers on how to use mobile phones, mobile banking and digital security, who then trained their peers and neighbours. Similarly, Point of View supports queer activisits in Gujurat to become 'community digital trainers', where they train their peers in local languages on the specific digital rights issues that queer folk in the region face. Running these digital literacy workshops highlighted the need for information which is available in local languages, formats other than text, and for different levels of digital access. Responding to this need, Point of View launched 'TechSakhi', a digital safety omnichannel helpline service which is accessible via phone, WhatsApp, Facebook, and other channels, and is operated by women from the same demographics as Point of View's workshop participants.

Influencing Policy, Media and Community

Through its rigorous research, Point of View draws attention of civil society organisations, media, and policy makers towards everyday workings of the law in the field of gender and sexuality. For instance, in 2017, Point of View conducted a research 'Guavas and Genitals' where they studied 99 cases filed between the years 2015-17 on the charge of Section 67 of Information Technology Act, 2000 (the digital counterpart of obscenity provision present under the Indian Penal Code, 1860). The research found that this provision was being misused to criminalise political speech, for online harassment, crimes of consent, censoring artistic expression, and for punishing obscenity. The research made a strong case for popularising the use of Section 66E by police for punishing non-consensual circulation of intimate images as a violation of privacy and consent, instead of using the obscenity law of Section 67 of the Information Technology Act, 2000. It also demystified concepts of consent, culpability, and sexual expression, and it pushed for a more informed and non-stigmatising approach to policy making.

> *"Our sense of our experience on platforms, and what constitutes violence or harassment or abuse, is not aligned with platforms and their sense of what constitutes harassment and violence and abuse. So if you ask what to change, I would love it if we could really have a ground up, user-centred, understanding. Based on lived experience, not based on categories or words."*
>
> Bishakha Datta

Our principles in practice

Point of View uses storytelling to illustrate the **plurality** of survivor experiences - and the need for **plurality** in solutions, too. They promote **agency** by ensuring the informed consent of survivors in the way their stories are told, and by centering lived experience in everything they do. They particularly focus their work on the most marginalised communities in India, demonstrating a deep commitment to **equity**. By telling stories not only of harm but also of resistance, and offering tools and guidance to help people resist, they encourage **hope** for all.

4.3 The potential of policy: justice and care

Policy measures have an important role to play in tackling tech abuse. These policies can be used to provide recourse to harm, provide protections for survivors, and even support tech companies to play a better role in preventing TGBV in the first place.

Framing and development of policy is often a crucial step in societal recognition of an issue. Policy can be an indication of a cultural shift in our understanding and attitudes towards tech abuse. For example, in the UK, the Online Harms Bill, which was introduced in March 2022, not only raised public awareness of online harms but has also had a catalysing effect on dialogues around the gendered elements of online harm, the impact of disability, the role of pornography, media literacy, platform accountability, and more. Policies can be a powerful tool in shaping people's conception of how tech abuse manifests and its varied impacts on people, especially those who are already marginalised. As such, it is crucial that policy accurately reflects and responds to the experience of survivors.

An intersectional, survivor-centred and trauma-informed approach to policy should encourage more nuanced practices when it comes to tackling TGBV. Policymakers should be thinking broadly about how to address tech abuse and support survivors in a meaningful way at every level. This could mean:

★ Incorporating a deeper understanding of how technology is used and accessed by different people.

★ Acknowledging the multiplicity of lived experiences and varied ways in which tech abuse happens, ultimately highlighting and meeting the need for multiple and varied support mechanisms.

★ Developing legal definitions to avoid causing further harm to already marginalised communities.

★ Ensuring that tech abuse is treated as a form of GBV and considering the need for safe reporting mechanisms and protections for victims.

★ Cultivating a better understanding of how online violence can cause as much harm as offline violence and the myriad of ways in which trauma can manifest as a result.

★ Creating processes to ensure that survivors feel validated and supported.

★ Developing policies in a way that centres survivors and recognises them as experts in their own experiences.

★ Considering the accessibility of the language used in the policy and moving away from too much jargon or use of victim blaming language.

★ Building in the wider frameworks needed to ensure that survivors have access to the support which the policy seeks to offer them, such as ease of accessing mental health support.

★ Creating additional guidance and allocating appropriate resources for those who will be implementing the policy, including for training, outreach, and community support.

It is essential that laws and policies be constructed after thorough consultations with survivors who bring a diversity of identities and perspectives, and follow the application of an intersectional analysis. Governments should move towards an ecosystem of legal, social, and systemic responses that address different aspects of the survivor experience and allow survivors to craft individualised pathways to justice.

Finally, while beyond the scope of this guide, we should think about existing criminal and civil legal frameworks that address tech abuse, considering what restorative and transformative approaches may look like in this space. Exploring such community-led alternatives might open up new ways to centre sexual expression, autonomy, and consent while better highlighting the harms experienced by survivors situated at multiple intersections of marginality.

Design principles and applications

1. Safety

It is vital that we promote the physical and mental safety of survivors throughout the legal process. As policymakers, we should ensure that this is outlined in the policies themselves, as well as any accompanying frameworks and guidance that we develop. Sometimes this may look like building in actual safety measures, but at other times, it may include things like clear and accessible definitions or free survivor access to

support, all of which shape the ways in which survivors can feel safe while engaging in a legal process.

Application examples:

★ Ensuring that policies include clear wording that allows survivors to identify the purpose of the policy, as well as the potential remedies available. This may mean refraining from using jargon which may confuse or alienate survivors and producing further guidance which explains and breaks down the law for those who are implementing it, as well as the general public.

★ Creating processes that allow for an iterative definition of TGBV, which potentially changes or grows over time to allow for the continuously new ways in which TGBV is perpetrated across new and old technologies.

★ Developing policy frameworks enabling free access to civil courts/processes for tech abuse cases so that survivors can have agency in leading their own process, unlike in criminal courts where the state is the main driver of a case.

★ Extending or dropping time limits on when a case can be brought. People react differently when they've experienced TGBV and they may not be ready to report incidents immediately. For example, several states in the USA are enacting legislation to create a 'lookback window' for adult survivors of child sexual abuse to access the civil legal system even when their criminal claims have expired because of statutes of limitations.

★ Categorising tech abuse laws within GBV laws and frameworks to account for the specifically gendered ways in which this harm often manifests.

★ Building in survivor-centred approaches for interactions with witnesses. These could include

  ☆ Asking survivors for safe contact details as these may differ from the ones that they use to report.

  ☆ Ensuring minimal communication between survivors and perpetrators during any criminal trial.

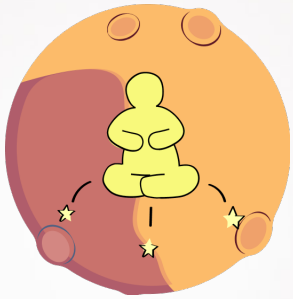
  ☆ Ensuring confidentiality of survivor details while reporting instances of abuse on tech platforms or with law enforcement agencies.

  ☆ Minimising emotional trauma of survivors by reducing the number of times survivors have to recount their abusive experience during trial. This can be done by recording one comprehensive statement that can be shared and used throughout all stages of the reporting process.

- ☆ Meeting survivors' needs through adequate non-legal support, including online and phone information, psychosocial support, and counselling that is accessible and relevant to the diversity of victims.

- ☆ Creating police/specialised reporting units that are adequately trained in trauma and tech abuse. This will help in preventing victim blaming or dismissing of cases due to lack of knowledge. As outlined in the Gender and IoT Research Report, this would require collaboration between cyber units and domestic violence services, as well as meaningful training, awareness raising, and resources allocated for all of this.

- ☆ Separating immigration from policing so survivors can access reporting processes without fear. There should be similar policies for sex workers or other.



2. Agency

We need our policies and frameworks to support survivor agency so that they feel free to choose their own path with the scaffolding of policies and practices in place. It is vital that survivors do not feel they are being forced to do anything, whether it's telling their story in a specific way, providing information they are not comfortable sharing, or even using language they don't feel safe using. This can mean actively seeking consent at various stages, keeping the survivors informed of their rights and their options, and actively seeking to serve the interests of survivors.

Application examples:

- ★ Drafting laws in a way that focuses on the survivor's consent (or lack thereof) instead of the perpetrator's intention.

- ★ Providing survivors with information on tech abuse and GBV support agencies during and post-report processes so that they know what help is available to them.

- ★ Building consent into various stages of the process, ensuring that the survivor knows how their information is going to be used and that they are able to opt out of the reporting process at any stage.

- ★ Providing survivors with the option to choose whether they wish to invoke criminal legal remedies; they should not be pressured into reporting to police. However, we must ensure that they are also aware of instances where this option cannot be given to them (in the case of imminent threats to their safety or of the public at large).

- ★ Ensuring that the survivor has civil law remedies as alternatives to criminal procedures.

- ★ Requiring all systems in which a survivor might find themselves after experiencing TGBV to be part of the solution through varied and tailored actions, such as setting up support centres, conducting training, and ensuring there is mental health support. For example, this may be offered in education systems that work with young people using technology to sext, or healthcare systems that work with survivors.

- ★ Clearly outlining complaint processes for handling cases, complete with external moderation processes where mediators or arbitrators are also adequately trained in consent, trauma, and TGBV generally.

- ★ Making independent third party reporting platforms available as a choice for survivors to access support.

- ★ Appreciating, thanking, and supporting survivors for their decision to come forward and report.

- ★ Providing survivors with information on tech abuse and tech abuse/ gender-based violence support agencies.

- ★ Educating all prosecutors and judges on sexual abuse trauma through mandatory trainings.

3. Equity

In creating equitable policies, we must embed accessibility considerations into our policies and their frameworks. Here, we mean accessibility in the broadest sense. We must ensure that we consider the experiences of marginalised groups and how they are likely to experience and understand abuse, and address this within policies we create.

Application examples:

★ Providing free legal assistance, support, and counselling to survivors and individuals from low-income and marginalised communities.

★ Creating policy guides to help survivors (and support workers) navigate the suite of tech abuse policies and help them identify which ones may apply to their situations, (such as the Australian Government's eSafety Guide).

★ Allowing third party reporting (for example, reporting by friends, family or support workers) with a survivor's consent.

★ Embedding interpreters throughout the process for those who are more comfortable interacting in a language other than that used by the courts, police and/or prosecutors.

★ Allowing individuals to report abuse in multiple languages through both online and offline modes that have the option of reporting in writing or orally, such as the India Cyber Crime Portal.

4. Privacy

Policies and frameworks should guarantee confidentiality throughout the process. This is essential for promoting other principles such as agency and safety. Often with tech abuse cases, the survivor loses control over their own information/images and how they are being shared. Strong privacy procedures must be in place for survivors to have confidence in the process.

Application examples:

★ Ensuring anonymity and confidentiality protections for tech abuse survivors as given under GBV laws and sexual assault shield laws, such as UK Special Measures and India's Rape Shield laws.

★ Prohibiting media from disclosing the identity of tech abuse survivors and supporting and amplifying trauma sensitive reporting practices.

★ Protecting and withholding survivors' personal details, from perpetrators in particular. Any right to confront a witness is done within a safe court setting, and with the support of an advocate/support worker upon the survivor's request.

★ Informing survivors of who is working on and/or has knowledge of their case within a legal or support team, and giving survivors the opportunity to withdraw consent to sharing further details of their case.

5. Accountability

Policymakers have the ability to build accountability into the process by how they frame obligations and who they address through them. It is important to consider not just the direct perpetrators of the harm but also those who can play a role in addressing it, such as law enforcement, platforms, tech companies, website hosts, and others. It is important to consider what mechanisms are built in to hold policymakers accountable themselves.

Accountability also means ensuring reporting mechanisms are clear and transparent, as well as open to receiving feedback for improvement. A key aspect of this would be contributing to reporting and research regularly, including collecting meaningful data. Additionally, policymakers often have good opportunities to influence budgets and could work to increase resource and capacity-building for those working directly with survivors on a day-to-day basis.

Application examples:

★ Placing a legal duty of care on tech companies across the distribution chain to ensure that they have adequate infrastructure to prevent tech abuse and to support survivors.

★ Setting a minimum regulatory standard for the industry to have specific processes in place to manage TGBV, with penalties for tech companies that do not meet these.

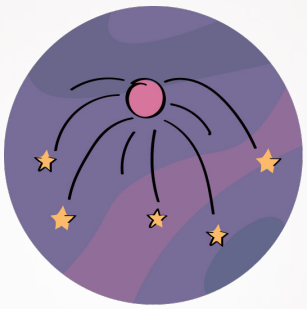
★ Developing feedback loops and consultations to allow ongoing input from survivors and the public on existing and new policies related to tech abuse.

★ Laws recognising the cross-border dimension of tech abuse and having provisions on how to navigate this borderless crime through agency collaboration and international law. There are perpetrators who live outside the country when engaging in tech abuse, and this must be accounted for in laws.

★ Setting clear requirements around data collection, which centre the survivor's agency, trust, and consent.

★ Increasing resources and capacity to properly equip those who implement these policies - such as law enforcement agencies, support services, and local governments - so they can support survivors.

★ Acknowledging and creating sustainable mechanisms to address the ongoing traumatic effects of tech abuse through the justice process in order to contribute to healing and accountability.



6. Plurality

Survivors are not a homogenous group so we must account for a multitude of different experiences in our policies and accompanying frameworks. Our legislation should incorporate the diversity of survivor needs and how their varying identities may impact their access to reporting.

Application examples:

★ Providing guidance and training for judges and law enforcement on the ways in which tech abuse manifests and impacts different communities.

★ Providing civil remedies, including compensatory and punitive damages, which can be sought through tort actions for the invasion of privacy and the intentional infliction of emotional distress. Tort actions can provide a more individualised determination of the harms, and offer tailored damages.

★ Supporting community leaders and maintaining that specific service providers for specific marginalised communities (such as those for LGBTQ+ people, Black people, people of colour, etc.) are well resourced, rather than amalgamating all services into one generic, centralised body.

★ Training those who implement policy on intersectionality and the ways in which harm can be compounded when someone is sitting at multiple sites of oppression.

7. Power redistribution

As policymakers, it is powerful to include processes which are participatory. This is a crucial step in redressing power imbalances that are present within our societies and often are exacerbated for survivors of tech abuse. We want survivors to have ownership of the processes that affect them, so that we can end cycles where survivors are subjected to laws, policies, and frameworks that don't reflect their needs and experience.

Application examples:

★ Making space and allocating resources to support survivors who want to lead drafting or inputting on policies and laws that affect them.

★ Ensuring that processes and frameworks are co-designed by survivors.

★ Communities are consulted through different stages of policymaking.

★ Enabling support workers to effectively work with survivors by providing funding and resources, including specifically on tech abuse training.

Mary Anne Franks drafted the first model statute on non-consensual porn. Working with survivors and being led by their expertise, this statute was informed by the knowledge and experience of survivors. This model statute has since been used as a template to amend their laws around non-consensual porn.

8. Hope

Policies need to ensure that the processes created to support survivors also validate their experiences and give them a sense of hope. It is essential that people's humanity is affirmed throughout, and they're reminded that their abuse does not define them. Our processes should leave survivors feeling supported and affirmed.

Application examples:

★ Creating and funding survivor assistance helplines that can provide immediate counselling, resources, and legal assistanceadequate infrastructure to prevent tech abuse and to support survivors.

★ Offering funding pools that have no specific deliverable. Survivors are not a monolith and each person has unique needs, so funding streams which address those unique needs must also be flexible and responsive.

★ Ensuring personalised and trauma-sensitive redressal to create an environment of trust and hope for survivors.

★ Creating human-centred and warm processes for grievances, complaints, and support. We must ensure that survivors feel taken care of and seen throughout the process.

★ Making other forms of healing available, beyond the court system, such as acknowledgment of the harm, apologies, or mechanisms enabling offenders to understand their wrongdoing.

★ Ensuring that all systems which survivors must go through are engaged and considered in creating a seamless policy that looks at both support and prevention. This includes the social service system, the health care system, the education system, and administrative (workplace) spaces. Experts from within these spaces are included in the policymaking process.

Case Study:

A collective of women's rights organisations: The Survivors' Agenda

Five years after the rise in the '#MeToo' movement in October 2018, a USA-based collective of 21 organisations and 60+ community partners who believed in the power of survivors to shape policy came together to create The Survivors' Agenda.

The Survivors' Agenda is a community-driven guide towards survivor justice. Led by those who have experienced sexual abuse and other forms of sexual violence, it is also a guide for those seeking to prevent and interrupt sexual violence, including sexual harassment. While it does not focus on TGBV alone, it is a powerful example of how survivor-led processes for policy making could work.

At its core, The Survivors' Agenda seeks to listen to survivors and put them at the centre of enacting institutional and policy change.

> *"Survivors of sexual violence, particularly survivors of colour, hold the answers when it comes to addressing and eradicating these problems. We know what reallocating funds within over-policed communities could do for survivors and their communities; it means that service providers would have the most up-to-date information about the communities they serve and the resources to respond to their needs. We could actually focus on prevention in schools with consent education curricula and offer comprehensive and culturally-sound mental health and social services."*
>
> Tarana Burke, Founder, #MeToo and Mónica Ramírez, founder, Justice for Migrant Women

Bringing survivors together

The Survivors' Agenda was born out of the need for survivors to lead the conversation about sexual violence and public safety in the USA. It sought to centre the most marginalised in the movement to end sexual violence, acknowledging that interlocking systems of oppression is a critical element toward collective healing and systemic change.

In September 2020, thousands of survivors and advocates convened at the Survivors' Agenda Summit, with three days of workshops, performances, and critical conversations to change the national conversation on sexual violence. The aim of the summit was to build collective power and grow a culture of care, safety, and respect for all.

For months prior, the collective had been crowdsourcing information about key issues, policies, and support that survivors had been calling for in order to build a collective vision. A set of policy demands was also created through a survey which garnered 1,100+ responses. They also brought together a group of 40+ individuals from their steering committee and community partner organisations to meet weekly from July to September 2020, to accumulate decades of expertise directly from those building the movement to end sexual violence.

In addition to the summit, there were also a number of virtual town halls, kitchen table conversations, and workshops for specific communities such as the Survivors' Agenda Virtual Town Hall for Survivors of Childhood Sexual Violence. Spaces like these provided an opportunity for robust participation of survivors, allowing them to share their insights, ideas, and thoughts on what is working in their communities, what needs urgent attention, and how survivors and allies can work together towards a world free and safe from sexual violence.

The agenda itself contains a number of powerful policy recommendations which will move us forward with tackling sexual violence. These include:

★ Prioritising community safety and providing alternatives to the criminal legal system.

★ Meaningfully shifting our culture through education.

★ Enabling better access for survivors to support and services.

★ Making healthcare, housing, and transportation more accessible for survivors.

★ Guaranteeing safety for workers across sectors.

Our principles in practice

The Survivors' Agenda actively reassigns **agency** and **redistributes power** to survivors by creating a process through which they can control the narrative and inform what is needed at a policy level. Importantly, they lean into the **plurality** of experiences by making it clear that they welcome and hold the experiences of people at any point along their survivor journey, as well as those who may not necessarily self-identify as such.

Similarly, there is a recognition that the world, as it currently exists, is not just. There needs to be an active effort to centre the voices and experiences of those most marginalised by the intersections of gender-based violence, white supremacy, and capitalism. As part of this, they also consider how imperialism, colonisation, enslavement, casteism, and genocide have created conditions for assault and violence on Black people, indigenous people, people of color, queer, transgender, intersex, and gender non-binary people, young people, workers, immigrants, those who are disabled, those currently or formerly incarcerated, and other historically marginalised groups globally. In centering these experiences, they are able to ensure their policy recommendations do not default to just one experience of survivorship and instead advance **equity**.

While holding virtual spaces, they also were intentional about the spaces they held and mindful of how to make them both safe and accessible, incorporating disability justice values and providing resources and support for those who may be impacted by the discussions.

Finally, it is a deeply powerful demonstration of **accountability** that the collective chose to say that the agenda itself is "a work in progress and a snapshot of what is needed to bring about transformation. The policies listed...are building blocks toward this transformation, but do not necessarily capture the entirety of the change we need." Ultimately, recognising that there is no one perfect policy outcome, The Survivors' Agenda provides hope to survivors and advocates that meaningful change is possible without essentialising or collapsing the survivor experience.

"Listening to survivors does not mean that people should 'study' survivors or 'interview' Black people who have been made vulnerable to both state-sanctioned and sexual violence because of their race. Instead, survivors of colour should be leading these conversations, proposing the solutions, and they should be empowered to create the vision of what a safer world looks like. Survivor voices—particularly those of Black women, trans women, and other women of colour—have been silenced and overshadowed for far too long."

Tarana Burke and Mónica Ramírez

5 Further explorations

Through the Orbits journey, we've discovered the complexities of tech abuse and survivor experiences around the world, and explored the failings of current systems and interventions in dealing with TGBV. Following this, we generated ideas of more nuanced, impactful solutions through using an intersectional, survivor-centred and trauma-informed approach. Coming to the end of the Orbits voyage, it is clear that this is just the beginning of the quest to truly tackle tech abuse. While we have presented principles to support taking such an approach, and offered examples of putting them into practice, much more work is needed to model, test, implement, and scale effective interventions and achieve the systemic change that we need.

We highlight the following areas of priority for further exploration:

Good practice case studies

We identified several cases of intersectional, survivor-centred, and trauma-informed interventions to tech abuse, and highlighted these in the case studies placed throughout the guide. However, these interventions largely come from civil society, and we struggled to find good practice examples of policy or technology design from mainstream platforms. We need to collect and collate more examples that demonstrate good practice in alignment with our principles.

Putting the Orbits principles into practice

The Orbits guide and principles are made to be used! As practitioners work with this guide and its core principles, we must gather insight into how they work, or do not work, and create more examples to demonstrate the values of intersectional, survivor-centred, and trauma-informed approaches.

Looking to the future

As TGBV continuously develops, Orbits can be used to anticipate, respond to, and design prevention/mitigation measures for new and emerging forms of tech abuse. For example, there is a pressing need for work on TGBV related to the metaverse and NFTs.

Applying the Orbits lens to other fields

Orbits focused on three areas that are vital to tackling tech abuse and align with the expertise of Chayn and End Cyber Abuse: technology, research, and policy. However, we know that the interventions that are needed extend far beyond these fields. We encourage those working on tech abuse from other sectors or vantage points to work with this guide and explore if and how it could support progress in those areas. For example, what might the Orbits approach look like when applied to communications or campaigning? What could frontline services for TGBV survivors using this guide look like? How can we build educational programmes based on these principles?

Data, data and more data

While there has been an incredible amount of thorough, informative research on tech abuse, data about the impact of different interventions is hard to come by. If we are to scale interventions that will actually create the transformations we require, we need data to demonstrate accurately what works and what doesn't. This is particularly true of the Global South, as

while writing this guide we came across far more recent research from the UK and the USA.

A basis for collaboration

Producing Orbits was a global, collaborative effort, but addressing tech abuse will require even wider, deeper collaboration and movement building. We'd love to explore how the principles and ideas suggested in Orbits could serve as a unifying tool for such a movement - providing a shared vocabulary, approach, and call to action.

6 Conclusion

Technology-facilitated gender-based violence is a problem that is as urgent as it is complex. As huge as it is nuanced. As fast-changing as it is multi-faceted. Addressing it requires many different interventions and global, cross-sector collaboration from governments, technology companies, civil society, and beyond. But to truly tackle tech abuse in a way that leaves no one behind, our interventions must be designed to be intersectional, trauma-informed, and survivor-centred. Solutions must serve all survivors and acknowledge the way TGBV interacts and intersects with other harms and forms of oppression, and impacts survivors differently based on other aspects of their lives and identities. Survivors, and their diverse experiences and perspectives, must be central to all interventions. We must acknowledge that TGBV creates severe trauma, and account for that in the design and execution of all remedies.

In Orbits, we've suggested eight principles that might help to design such interventions, focusing particularly on the fields of technology, research, and policy. We've looked at the different forms of tech abuse, and the harrowing impact it can have on survivors. We've explored how and why current approaches are failing, and started to sketch out what an alternative approach could look like. We've acknowledged that there are systemic issues underlying TGBV that require long-term solutions, but also that there are many, many immediate changes that technology companies, researchers, and policymakers can make now to better support survivors. We've given examples of what the principles look like when translated into practice and looked at case studies from around the world.

While the challenge of TGBV is undoubtedly a huge one, it is not insurmountable. We can build a world where technology and the internet promote (rather than threaten) safety, and where privacy is a right in practice. We can transform technological, political, and social responses to TGBV, and all forms of GBV in ways that give survivors agency and are based on equity for all. We can build solutions that show plurality, by responding to diverse experiences and contexts, and accountability, by being open, transparent, and responsive. We can kickstart power redistribution to create the systemic changes we need. For every survivor, we can, and must, have hope.

7 Glossary

Ableism: A system of oppression in which disabled people are discriminated against and marginalised.

Coercive control: A form of psychological abuse where a perpetrator seeks to control someone through a pattern of manipulative behaviour and actions.

End-end encryption: A method of secure communication, regarded as the gold standard, that prevents third parties from accessing data while it's transferred from one endpoint or device to another.

Extractive research: Research which takes information and knowledge from research subject(s) without care or regard for their wellbeing and preferences, or how the subjects themselves benefit from the interaction.

Gender-based violence: Harmful acts directed at an individual based on their gender.

Gendered: Reflecting gender differences or stereotypes.

Intersectionality: A term, coined by Kimberlé Crenshaw, to explain how people living at multiple sites of oppression can experience violence, harm, and discrimination in particularistic and compounded ways.

LGBTQ+: The acronym for lesbian, gay, bi, trans, queer, and other marginalised sexual and gender orientations. For a full list of included terms denoted by the +, see Stonewall's Glossary.

Patriarchy: A societal system where power is held by men.

Restorative justice: An approach to addressing harm by facilitating conversation between the person/people affected and the person/people responsible, rather than punishment.

Retraumatisation: When people re-experience past trauma and associated thoughts and feelings.

Remedies: The way in which a court of law enforces a right, imposes a punishment, or makes another court order to compensate for harm inflicted.

Technology-facilitated gender-based violence (also referred to in this guide as tech abuse): Harmful acts directed at an individual based on their gender which use or involve technology.

Trauma-informed: Practice which understands and acknowledges the nature and impact of trauma.

Survivor-centred: Practice which prioritises the experiences and perspectives of survivors.

Victim blaming: When someone who has experienced harmful or abusive behaviour is held partially or fully responsible for it.

8 Tools

The Orbits toolkit offers some ready-to-use tools for translating the Orbits tools into practice in your own work. They are all available under creative commons licence - feel free to use, adapt, and edit in your own work.

Tools for technology designers	An audit template to review your product or service against the Orbits principles and identify areas for improvement.
Tools for researchers	A template consent form, research FAQs, and after-research care package for working with survivors.
Tools for policymakers and advocates	A tool to scaffold your thinking when building policy interventions. Go to page 104.
Tools for movement builders and organisers	A template to design workshops based on the Orbits principles.

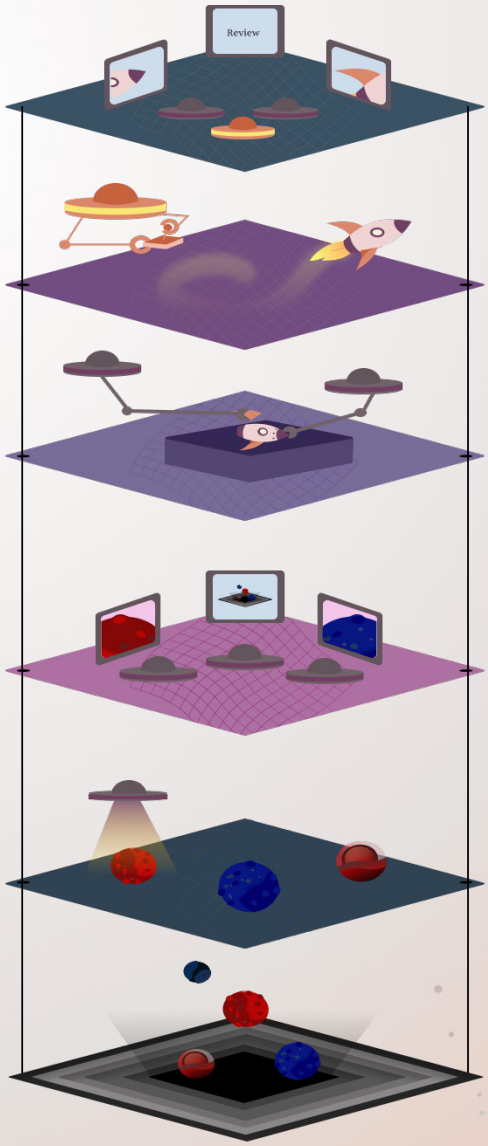
9 How to build policy using the Orbits principles

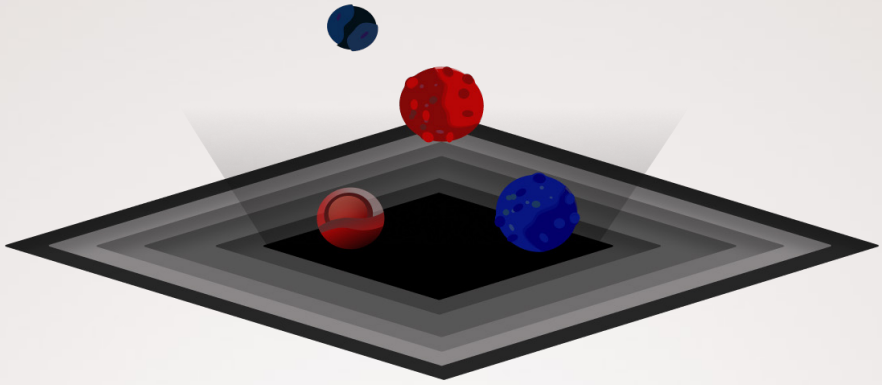
If real change is going to be possible at a policy level, it is not through a perfect policy outcome. You must consider how your institutional infrastructures for building policy are set up - how do the invisible structures of your legislative and regulatory systems work and can you uncover, explore and add nuance and complexity to this process (at least in your area of work)?

This tool will allow you to apply the interconnected Orbits principles as a way to scaffold building an intersectional, survivor-centred and trauma-informed approach to your tech abuse policy interventions. Ultimately, it provides you with a way to be reflexive and explore the multiple complex layers of policy building as you are engaging with it. This structure of this tool demonstrates:

- ★ How multiple activities may need to happen at the same time with different groups in different places and in different ways.
- ★ The diversity in the scale of what may be needed depending on your context.
- ★ The tangible and less tangible aspects of building policy.
- ★ A visualisation of how we often need multiple interventions, approaches and innovations around a problem.
- ★ How, as you move towards the foundations of the building, some aspects may be more challenging, long term or complex to shift.

In this tool, inspired by Visualising and Communicating Complexity by Dark Matter Labs, each layer of building a policy is mapped against a structure and supported by the scaffolding of example questions you may want to think about when coming up with policy interventions for technology-facilitated gender violence (TGBV). Feel free to add more questions in the spaces provided as you start to engage with this tool. We recommend you start from the bottom up!





Sociocultural context:

This is the overall context in which your policy is being built, including the range of social and cultural factors many of which are not immediately present, such as historical factors, systems of oppression etc. For example, in the context of TGBV, we might think of sexism, transphobia and homophobia, as well as the historical use of technology (e.g. Facemash). All of this gives meaning to any policy you're pulling together. Crucially, as policy-makers, you are not merely situated in a sociocultural context. You also help shape the context. It would require a sustained long-term investment and effort to change this context.

Questions to consider:

★ How will you consider the impact of systemic inequities and the wider sociocultural context in your country when drafting your policy?

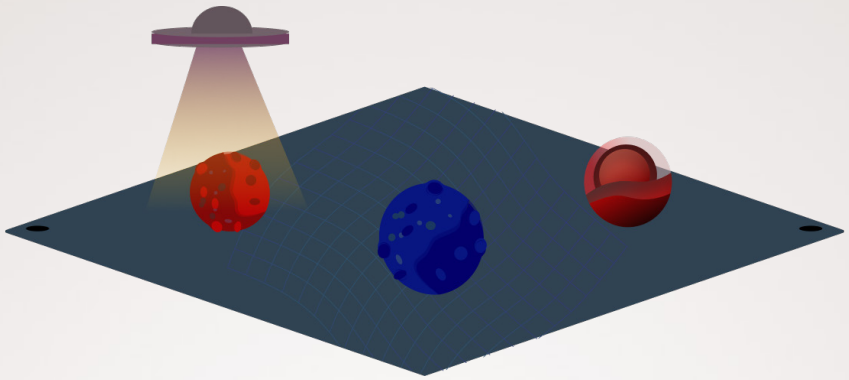
★ How will you ensure your policy is inclusive of and accessible to marginalised communities and individuals in your country?

★ How will you ensure you are avoiding racial, gender, class or other stereotyping happening when your policy is implemented?

★ What other ways will you consider equity when designing your policy?

★ Add your own question.....

★ Add your own question.....



Agenda building:

Before a policy can be created, problems must be identified and be called to the attention of the government and you, as policy makers. This is often the stage where the challenge is laid bare for you to address and come up with solutions. There can be many things competing for attention here and, often, the agenda may be driven by the concerns of the day. This is where the sociocultural context might impact the agenda. However, individuals also have the power to shape, push and mould the agenda.

Questions to consider:

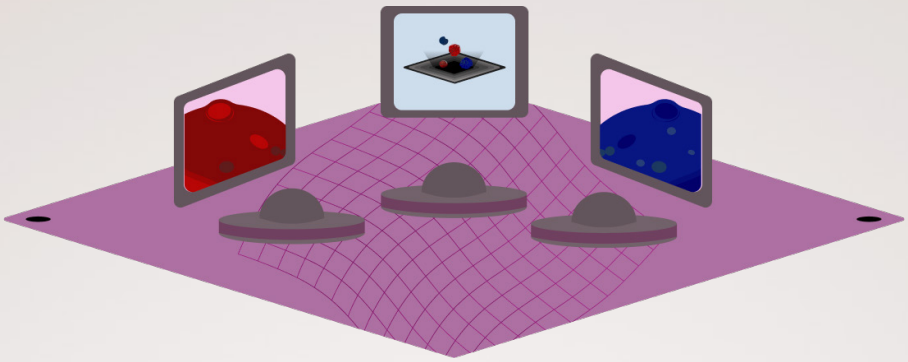
★ How will you include survivor representatives in the process of understanding the issue to better draw from their lived experiences?

★ How will you ensure you have the information you need to anticipate and respond to different needs and preferences of different communities?

★ Are there ways in which you can support community-led action to bring certain topics to the attention of the government?

★ Add your own question.....

★ Add your own question.....



Policy formation:

Once you've understood the situation, this is where you're coming up with different courses of action as approaches to solving the problem. This may include development of policy options, debates, consultations, public or government readings, reviews etc. Usually the executive branch of government is involved in this, along with perhaps the courts and interest groups. The way this happens depends on the legislative process in your country. The process itself may be changed but it may take time.

Questions to consider:

- ★ Will your version of the policy prioritise physical and emotional safety of a survivor? How?
  - ☆ If not, do you need to consult a group of experts on how to do this?
- ★ Have you thought about survivor consent when it comes to participating in any process you include in this policy?
  - ☆ Will your consent processes facilitate consent which is voluntary, informed and reversible? How?
- ★ Will this policy interact with privacy laws and regulations to shield the confidentiality of survivors?
  - ☆ Will you ensure that only the information that is absolutely necessary is collected, creating clear, optional options for more data?
- ★ Will your policy enable survivors to tailor any processes and support to their own needs and preferences?
  - ☆ Will they be enabled to describe their own experience and share the remedial measures they wish for, rather than forcing reports into rigid, predetermined categories?
- ★ Have you referenced (or built the creation of) bodies that can support a survivor through any legal process?

- ☆ Will this policy allow for free legal assistance, support and counselling to survivors and individuals from low-income and marginalised communities?
- ☆ What other ways have you considered survivor agency in your policy?

★ Should there be additional guidance that accompanies this policy to ensure it is accessible and implementing bodies are fully resourced to support survivors in a holistic way?

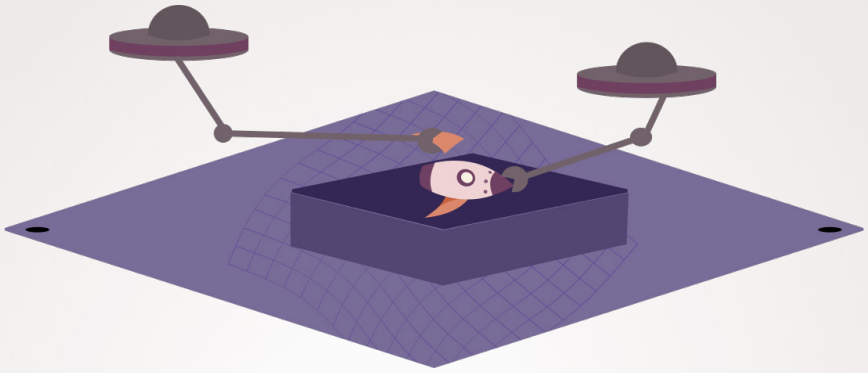
★ Would a civil process be more suitable and supportive of a survivor here than (or in addition to) a criminal one?

★ Is there a way to include survivor-advocates who want to lead drafting or inputting on this policy?

★ Does this policy ensure that different bodies are working in unison, not siloes? Such as, engaging all the systems survivors find themselves in after experiencing sexual violence - social service system, health care system, education system, administrative (workplace) system.

★ Add your own question.....

★ Add your own question.....



Decision making:

Government single out a particular course of action towards the remaining policy choices, thinking about what is for the greatest public benefit. This decision itself is often centralised but there are options which have, hopefully, been shaped more widely.

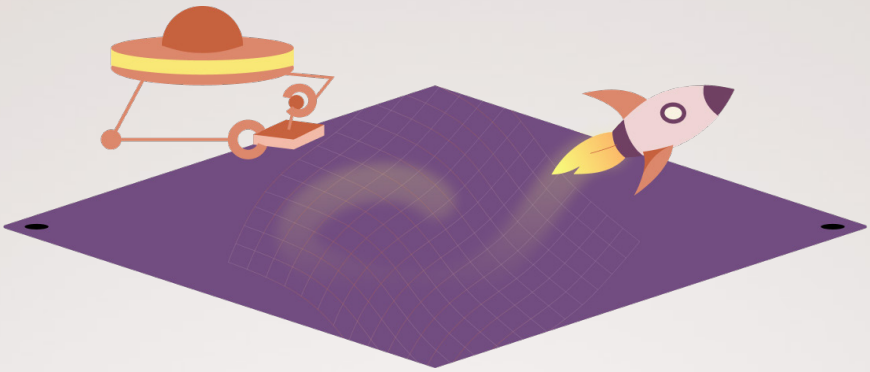
Questions to consider:

★ Will the decision making process prioritise survivor expert testimonies and lived experiences?

★ What pathways will be available if survivors and experts want to contest a decision?

★ Add your own question.....

★ Add your own question.....



Policy implementation:

This is when you roll out the policy and through public administration tools, officials, resources etc. These people are often not the same people who formulated the policy itself. There are different levels of flexibility in implementation depending on how clear the policy is, the resources applied, existing knowledge levels, the sociocultural context etc.

Questions to consider:

★ Is your policy clearly and easily worded so it can be implemented seamlessly, even by those who may not have heard about TGBV before?

  ☆ If not, can you provide further support and guidance to those who will ultimately be implementing it so that survivors are not subject to further harm?

★ Can extra resources be created to make the policy easy to understand by the average person?

★ Will you include training on the impact of additional vulnerabilities (like that of caste, race, religion, sexual orientation, and disabilities) on survivors' experiences for those who are implementing the policy?

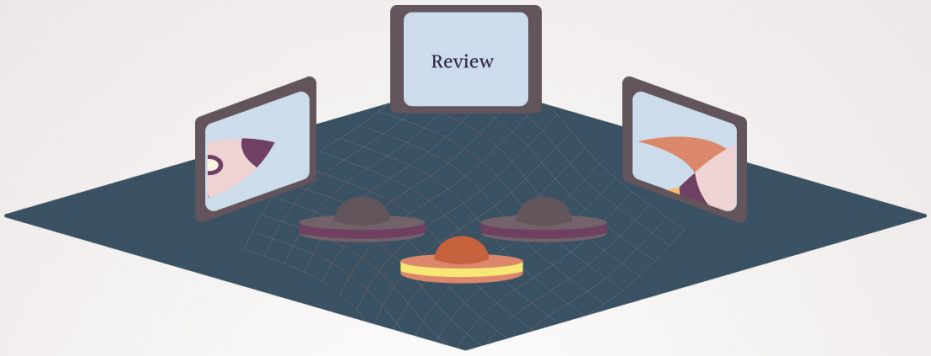
★ Will the processes arising from this policy cater to a range of accessibility requirements such as speech and hearing impairments?

★ Are there multiple ways for survivors to seek support for the rights outlined in this policy? For example, online portal, calling, in person etc.

★ What do the processes arising from this policy look and feel like for survivors'? Are they human-centred, warm and hopeful?

★ What have you done to reduce the risk of retraumatisation for survivors who will be impacted by this policy?

★ Add your own question.....



Policy evaluation:

Once a policy is live, it is reviewed for its effectiveness. This doesn't mean it will be repealed (this is generally difficult to do once in place) but amendments may be proposed in the future or it may impact future decision-making.

Questions to consider:

★ Are you building in ways to measure whether this policy actually works?

★ How does your evaluation process give power to and listen to those who may be impacted by it?

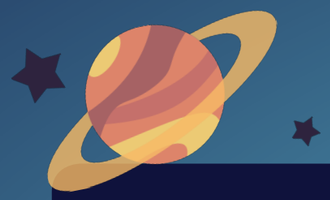
★ How will the learnings be fed back into future changes and how will policy makers be held accountable to that?

★ Add your own question.....

★ Add your own question.....

10 Orbits library

We have referenced amazing initiatives that we've learnt from, worked with, and been inspired by throughout Orbits, but there are many more - an entire ecosystem of changemakers is working towards a better future for survivors and a planet free from TGBV. Here are some fantastic resources, toolkits, and research we have at our disposal.



Resources for survivors

★ End Cyber Abuse has compiled a list of country-specific resources for survivors of tech abuse.

★ Chayn's DIY Online Safety guide provides practical guidance on staying safe online. Written particularly for women dealing with domestic abuse or stalking, the tips contained in the guide are useful for anyone who wants to tighten their online security. Both a starter pack and advanced version of the guide are available.

★ Maru is a chatbot to support people dealing with online harassment and abuse.

★ Safe Sisters is a graphic guide on digital safety for women and girls in sub-Saharan Africa.

★ StopNCII.org is a joint initiative from the Revenge Porn Helpline and Meta, offering a preventative tool to stop the sharing of non-consensual intimate images through innovative technology. The Revenge Porn Helpline has also collated a directory of support around the world here.

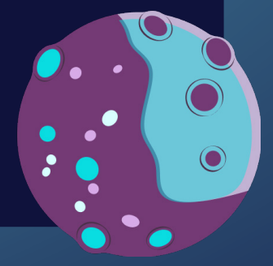
★ The Cyber Civil Rights Initiative provides comprehensive advice and support to survivors in the USA.

★ The School of Sex Ed in the UK has produced a guide on online sexual harrassment for students.

★ Powersingh's OGBV toolkits empower survivors by helping them to better understand technical and legal responses to OGBV.

★ The Cybersmile Foundation provides help and support to anyone experiencing cyberbullying, including TGBV.

★ End Tab has published a safety guide on non consensual tracking and personal trackers



Tools and campaigns for action

- ★ Glitch's Toolkit is for anyone who wants to play their part in ending online abuse by facilitating conversations about the problem in their networks and communities. The original Toolkit 1.0 is available here and Toolkit 2.0, focused specifically on taking action on online abuse against Black women, is available here.
- ★ Take Back the Tech is a global campaign to end TGBV.
- ★ The Trust and Abusability Toolkit provides tools for support workers, educators, journalists, researchers, and technology developers to promote safer technology. It focuses on the concepts of abusability and trust, showing that in order to build safer tech, we must anticipate how it can be abused, and question if and why people should trust technology.
- ★ #NotYourPorn is a campaign holding the porn industry accountable for the distribution and commercialisation of non-consensual intimate images.
- ★ EndTAB, led by Adam Dodge, provides staff training and community and student presentations on tech abuse.
- ★ FMA offers tools to fight online gender-based violence.

TGBV around the world

- ★ Learn more about tech abuse around the world from the International Center for Research on Women's TGBV research hub.
- ★ Global Citizen tells the story of three survivors from different parts of the world.
- ★ Tech Vs Abuse, a joint report from SafeLives, Snook, and Chayn, examined the state of tech abuse in the UK in 2017.
- ★ Pollicy's report Alternate Realities, Alternate Internet investigates OGBV in Ethiopia, Kenya, Senegal, South Africa, and Uganda.
- ★ Learn about how to end TGBV in Africa through this ten-point strategy.
- ★ Read about smart-home abuse in the USA in this investigation by the New York Times.
- ★ My Life is Not Your Porn is a study from Human Rights Watch looking at the devastating impact of digital sex crimes in South Korea.
- ★ KICTANET's A Safer Web for Women comic strip illustrates what tech abuse can look like for women in Kenya.
- ★ Learn more about how online abuse impacts women in their working lives in Australia.

Deeper dives

★ The Emerald International Handbook of Technology-Facilitated Violence and Abuse is an open-access, multidisciplinary ebook exploring TGBV and its possible solutions around the world.

★ In addition to producing regular research, University College London's Gender and the Internet of Things project publishes a monthly newsletter highlighting academic research and news on TGBV.

★ What does building an intersectional feminist internet look like? Read an edited version of Waag's 2022 State of the Internet lecture by Nani Jenson Reventlow.

★ IT for Change's Feminist Observatory of the Internet project creates space for nuanced debates and discussions about feminism and the internet, including issues related to TGBV.

★ Trust Through Trickery is a research study on harassment in messaging apps and explores what design elements facilitate harassment.

★ #ShePersisted's research takes an in-depth look at violence against women in politics.

★ Demos' Silence, Women investigation looks at gendered attacks online, while their report Engendering Hate looks at how gendered disinformation is used to exclude and undermine women in public life.

★ GLAAD's Social Media Index is the world's first baseline evaluation of LGBTQ+ safety on social media.

★ APC's white paper on feminist internet research explores feminist internet research, with a focus on scholarship from the Global South.

11 Acknowledgements

This guide was shaped and inspired by thinkers, doers, designers, creators, activists, and more from all around the world. To everyone who contributed - thank you. Orbits is a result of your insights, passion, and expertise. Below is a list of many incredible minds that contributed to Orbits. There are several others who opted to remain anonymous.

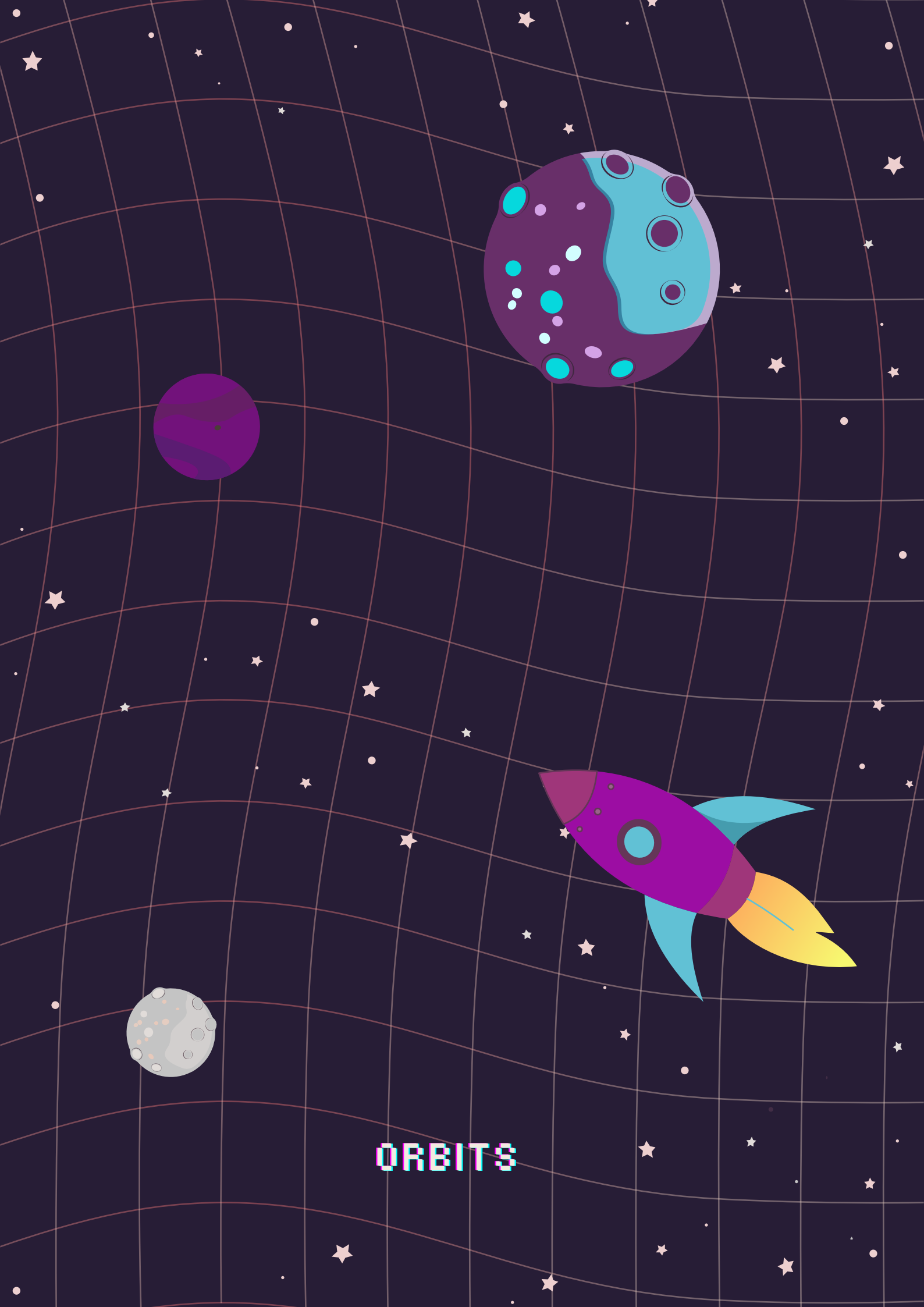
★ Garnett Achieng
★ Chioma Agwuegbo
★ Jackie AKello
★ Kim Barker
★ Lulú Barrera
★ Vaibhav Bhatla
★ Gayatri Buragohain
★ Chenai Chair
★ Yasmin Curzi de Mendonça
★ Nighat Dad
★ Debarati Das
★ Bishakha Datta
★ Maggie Delano
★ Azmina Dhrodia
★ Suzie Dunn
★ Sarah Fathallah
★ Mary Anne Franks
★ Jessica Gottsleben
★ Tara Hairston
★ Justin Henck
★ Elsa Hestriana
★ Anna Hughes
★ Suzanne Jacob
★ Katambi Joan
★ Ellen Judson
★ Fabrice Kaburugutu
★ Shmyla Khan
★ Eve Kraicer
★ Christina Lopez
★ Chiara Marinelli
★ Cecilia Maundu
★ Alex McCarthy
★ Clare McGlynn
★ Fatima Mehmood
★ Elena Michael
★ Peter Mmbando
★ Kiki Mordi
★ Sharon Muriuki
★ Chanelle Murphy
★ Eva Penzey Moog
★ Audrey Putz
★ Nissa Ramsay
★ Dama Sathianathan
★ Madeleine Ray
★ Koninika Roy
★ Ledys Sanjuan
★ Cielito Saravia
★ Leonie Tanczer
★ Mariana Valente
★ Charlotte Webb
★ Sarah West
★ Jenny Winfield

Contact Chayn **team@chayn.co**, or find us on social media:

facebook.com/chayn
twitter.com/chaynhq
instagram.com/chaynhq

Contact End Cyber Abuse on **hello@endcyberabuse.org**, or find us on social media:

facebook.com/endcyberabuseorg/
twitter.com/end_cyberabuse
instagram.com/end_cyberabuse


ORBITS