ORBITS

Policy chapters

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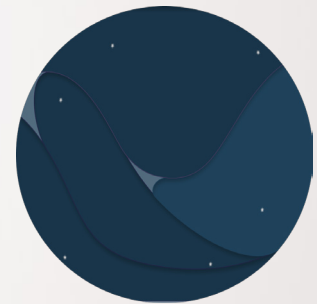
appropriately have their complaint addressed when harm does occur. It also offers more loopholes for perpetrators to evade the law and take advantage of different levels of regulation in different countries to perpetrate harm.

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.
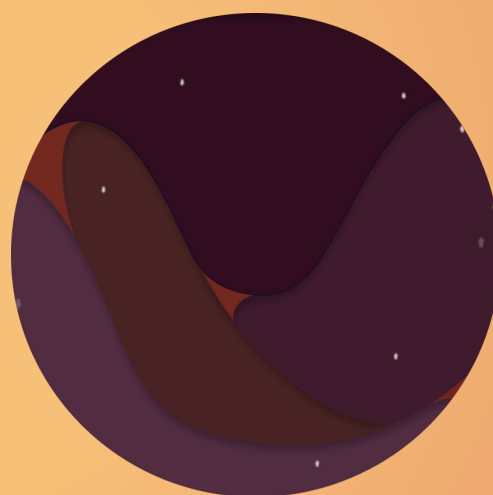
Case Study:

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

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
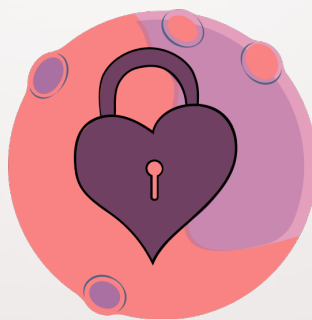

1. Safety

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 criminalised statuses and professions so that they may access support without fear of retribution.
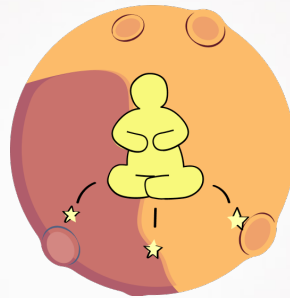
2. Agency

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 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.
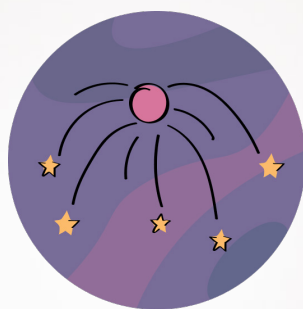

6. Plurality

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.
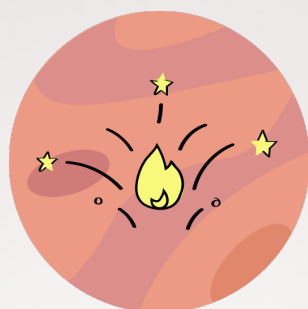
7. Power redistribution

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.

★ Consulting communities 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 assistance adequate 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 <u>USA-based collective of 21 organisations and 60+ community partners</u> who believed in the power of survivors to shape policy came together to create <u>The Survivors' Agenda</u>.

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."

<u>Tarana Burke, Founder, #MeToo and Mónica Ramírez, founder, Justice for Migrant Women</u>

<u>Bringing survivors together</u>

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 <u>build collective power and grow a culture of care, safety, and respect for all</u>.

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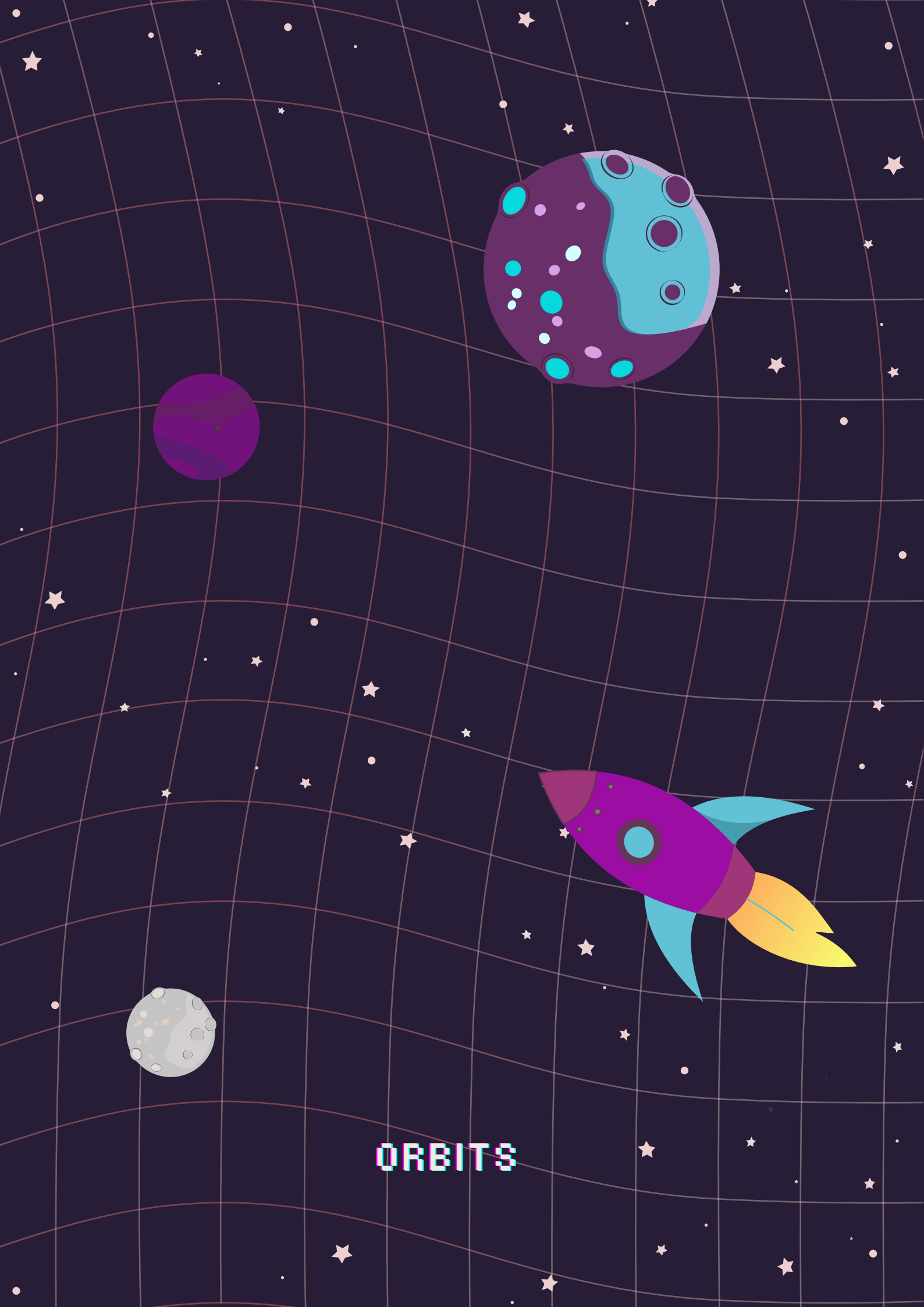
While holding virtual spaces, they also were intentional about the spaces they held and mindful of how to make them both safe and accessible, incorporating disability justice values and providing resources and support for those who may be impacted by the discussions.

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

ORBITS