ORBITS

Case studies

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 pops up 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.

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.

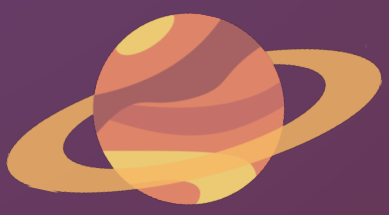
Our principles in practice

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

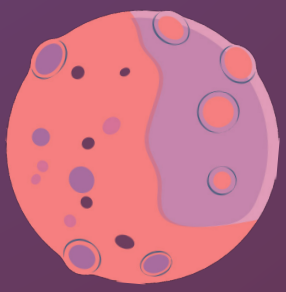
Case Study:

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**.



Case Study:

Bloom by Chayn - using tech to support healing

s 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.

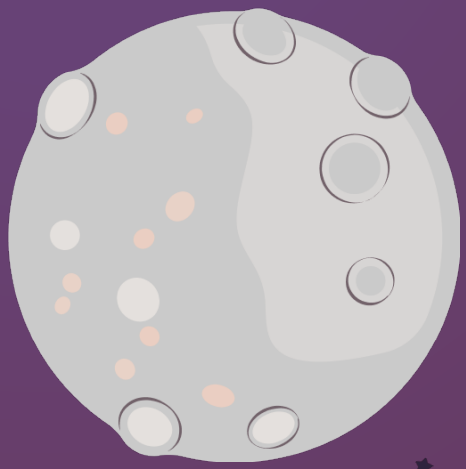
Curation	Reporting
1. Offering more granular settings (e.g. who can see, share, comment, or reply to posts) 2. Using simple and accessible language throughout the user experience 3. Providing easy navigation and access to **safety** tools 4. Reducing the burden on women by proactively reducing the amount 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.

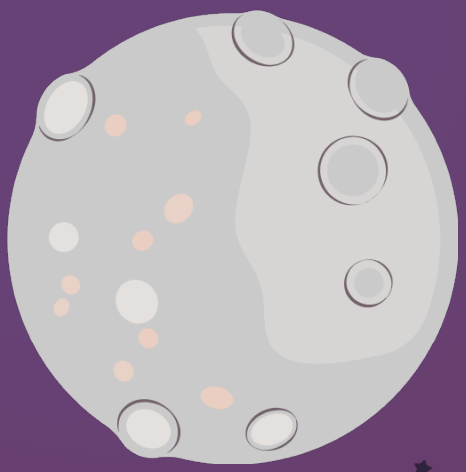
Alongside creating this tech, Pex has also begun community engagement work on the issue of IBA. Since IBA is a reflection of societal attitudes and prejudices, Pex sees a role for facilitating conversations to raise awareness about this topic, build solidarity and empathy for survivors, and shift the 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

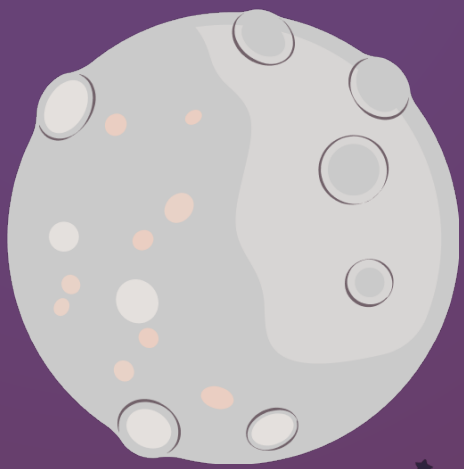
The helpline receives calls on many different types of online violence, including hacking, online stalking, doxxing, impersonation, and abusive language. However, their most common cause of complaint (around a third of overall calls to the helpline) relates to blackmailing: when threats and demands are 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.



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.

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.

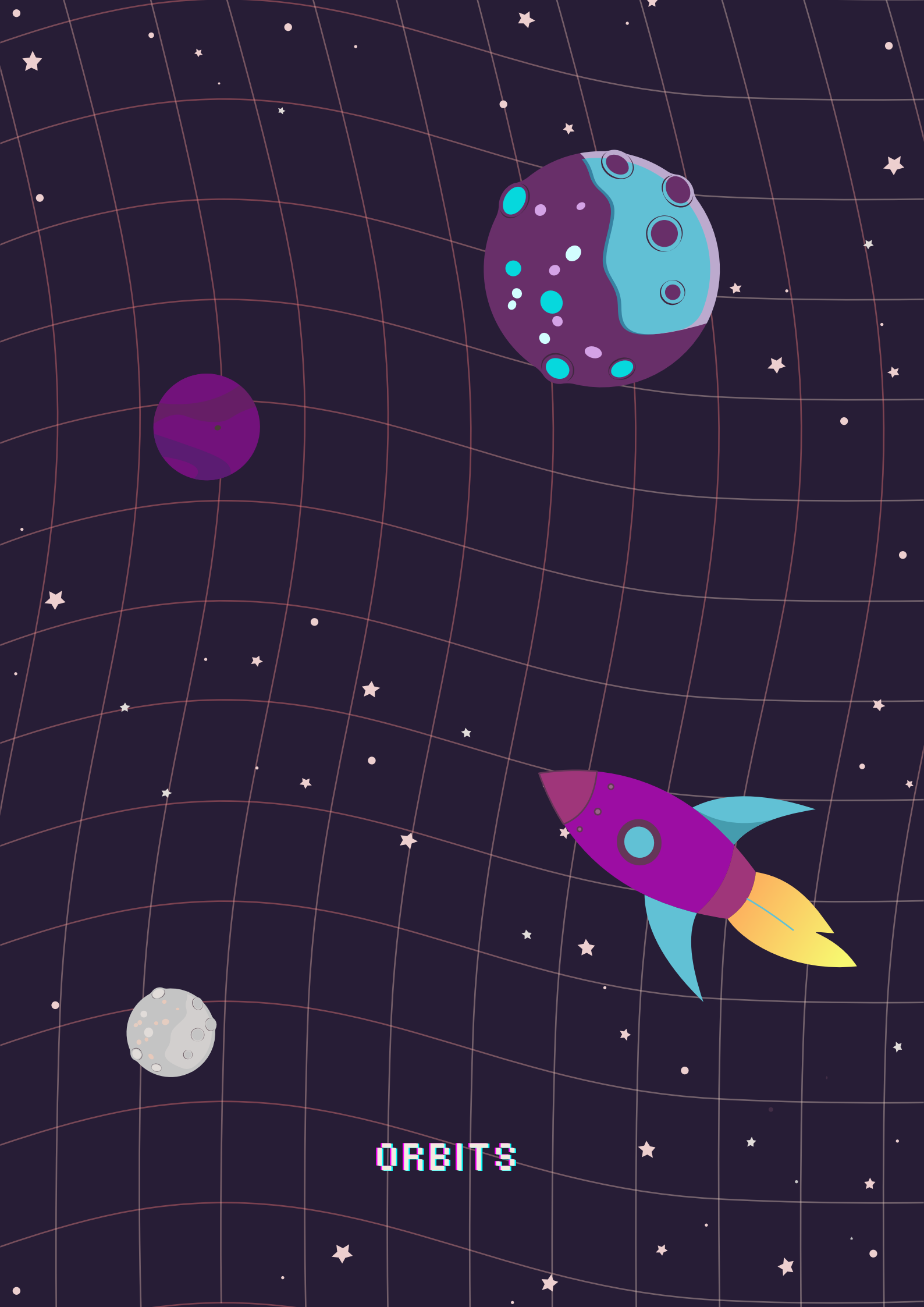
Similarly, there is a recognition that the world, as it currently exists, is not just. There needs to be an active effort to centre the voices and experiences of those most marginalised by the intersections of gender-based violence, white supremacy, and capitalism. As part of this, they also consider 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


ORBITS