**What is it?**
Age verification is a strategy used by online platforms to make sure that everyone who registers on the platform is above the legal age; however, the way that age is verified (providing passport or ID copies) is very problematic for sex workers.

**Threats:**
Providing passport or ID copies increases the risk of harassment, doxxing and other online and offline violence, particularly in contexts where sex work is criminalised.
Age verification requirements create barriers to entry for sex workers, particularly for those who are migrants and racialised, which can limit their ability to earn a living, potentially forcing them into less secure working conditions.

**Resistance:**
Sex workers can report instances of discrimination or harassment during age verification processes to advocacy organisations. Advocating for the development and use of self-verification tools or other alternatives where individuals can verify their age without disclosing sensitive information can help protect sex workers.
Advocating for platforms to adopt data minimisation practices, where only essential information is collected during age verification processes, can help reduce the harm of privacy breaches.
BIOMETRIC SURVEILLANCE
What is it?
Biometric surveillance is a practice based on collecting and analysing biometric data (fingerprints, voice, facial or gait recognition and iris detection) to monitor, identify and classify individuals.

Threats:
Biometric surveillance exacerbates the discrimination and criminalisation sex workers face by exposing them.
Biometric data can be misused or exploited, leading to breaches of privacy and further harm.

Sex workers will be reluctant to access essential services such as healthcare, counselling or legal aid if they fear that their biometric data could be used against them or shared with authorities.

Resistance:
Supporting legal advocacy efforts to challenge the use of biometric surveillance against sex workers and advocate for policies that protect sex workers’ rights to privacy, such as lobbying policymakers, participating in public consultations, and raising awareness about the harms of biometric surveillance on sex workers' rights and well-being.
What is it?
Cloud services store information over the Internet on a pay-as-you-go basis, replacing physical hardware such as USB sticks. These services are provided by cloud service providers, who host and manage infrastructure in remote data centres.

Threats:
Storing sensitive information, such as client communications, payment details, and personal identifiers on cloud services exposes sex workers to privacy risks.

Sex workers in locations where sex work is criminalised face legal compliance challenges when using cloud services. Providers may be subject to legal pressure to monitor, restrict or report sex work-related activities.

Resistance:
You can encrypt your data before uploading it to the cloud to protect it from unauthorised access.
You can review and adjust privacy settings on cloud services to control who has access to your data and how it is shared or displayed.
You can enable two-factor authentication (2FA) on cloud accounts to add an extra layer of security and prevent unauthorised access to accounts.
What is it?
Content moderation is the process of monitoring, reviewing, removing or restricting user-generated content (such as text, images, videos, and links), which can be done by humans or algorithms.

Threats:
Content moderation policies unfairly target sex workers, leading to the removal or restriction of their content or accounts.
Discriminatory content moderation practices directly impact sex workers' livelihoods, leading to economic harm.
Discriminatory content moderation practices exacerbate social isolation and prevent access to healthcare, legal services, peer support networks, and advocacy organisations.

Resistance:
Document instances of discriminatory content moderation, such as unjustified removal of posts or accounts, and report them to the relevant platform or oversight body.
Seek legal assistance and advocacy support to challenge discriminatory content moderation practices through litigation or policy advocacy. Human rights organisations specialising in digital rights, freedom of expression, and sex workers’ rights can provide resources and support.
Build alliances with other marginalised communities and civil society organisations to amplify voices and advocate for systemic change.
What is it?
Deepfake technology can be used to create realistic fake pornographic videos or images without the consent of the individuals depicted.

Threats:
Deepfake abuse can compromise the safety and security of sex workers by exposing them to potential harassment, blackmail, stalking or violence. The nonconsensual distribution of fake content may attract unwanted attention and threats from clients, acquaintances, or strangers.

Deepfake abuse undermines sex workers' autonomy and control over their own bodies and images, which can cause profound psychological harm.

Resistance:
Education on how deepfake technology works and common tactics used by perpetrators can help sex workers recognise and mitigate the risks associated with deepfake abuse.

Establishing clear communication with clients about expectations and limitations regarding using images and content can help reduce instances of deepfake abuse.

Advocate for legal protections and policy reforms to address deepfake abuse. This involves supporting efforts to advocate for platforms to implement policies and mechanisms for reporting and removing fake content.
What is it?
Digital payment services enable individuals to make financial transactions over the Internet or through mobile devices. These services facilitate the transfer of funds between parties without needing physical cash.

Threats:
Sex workers face discrimination from financial institutions and payment processors who freeze their accounts without warning, leading to financial instability and difficulties in accessing funds.

Sex workers are vulnerable to chargebacks and fraudulent transactions, where clients dispute payments or claim unauthorised use of their accounts to request refunds.

Resistance:
You can diversify your payment options to reduce reliance on a single digital payment service. You can use peer-to-peer (P2P) payment platforms that prioritise user privacy. P2P payments allow for direct transfers between individuals without intermediaries.

You can build support networks within your communities and allied organisations to teach and learn other strategies. You can advocate for legal reforms and policy changes to address discrimination, stigma, and regulatory barriers that limit your access to digital payment services.
What is it?
Intimate image abuse is the capturing and distribution of private or intimate images or videos of an individual without their consent.

Threats:
Intimate image abuse exacerbates the discrimination sex workers face. Victims face victim-blaming attitudes and are judged due to their involvement in sex work.
Perpetrators of intimate image abuse threaten to publicly share the images or videos.
Sex workers face additional legal vulnerabilities when dealing with intimate image abuse due to the criminalisation of sex work.

Resistance:
Practising digital hygiene, such as using encrypted messaging apps and virtual private networks (VPNs), strong passwords and watermarking, can help protect privacy and prevent unauthorised access to personal data and images.
You can build support networks within sex work communities and allied organisations to provide mutual assistance.
You can seek legal assistance from sex workers and victims’ rights organisations to pursue legal remedies against perpetrators.
You can advocate for platform accountability and tools to prevent intimate image abuse.
What is it?
Predictive policing is a crime forecasting strategy that uses algorithms to predict where and when crimes are likely to occur.
It relies on historical crime data, demographics, and other information to identify potential ‘crime hotspots’.

Threats:
Algorithms target areas where sex work is more prevalent, leading to heightened police presence and surveillance. This can result in increased harassment, arrests, and other forms of violence.
Predictive policing leads to the displacement of sex workers to other areas that are not targeted by law enforcement, pushing sex workers into dangerous locations where they have less access to protection.
The collection and analysis of data for predictive policing purposes is a threat to the privacy of sex workers.

Resistance:
Engage in advocacy efforts to challenge the use of predictive policing, such as lobbying policymakers, participating in public consultations, and raising awareness about the impacts of policing on sex worker communities.
Educate your community about their legal rights when interacting with law enforcement.
What is it?
Shadow banning is a form of content moderation by online platforms to restrict the visibility of a user's content or profile instead of explicitly suspending the user.

Threats:
Shadowbanning silences sex workers’ voices and limits their ability to share information, promote their services, or engage with their communities, resulting in loss of income and isolation.

Shadowbanning harms sex workers' ability to advocate for their rights and participate in online discussions, which limits their capacity to fight discrimination and harmful policies.

Resistance:
Be mindful of using keywords or hashtags that are commonly associated with adult content or sex work, which may increase the risk of shadowbanning. Consider using less explicit language when describing your services or content.

Avoid relying solely on one platform for your online presence. Diversify your online presence across multiple platforms to reduce the impact of shadowbanning on your visibility and reach.