nswp

Global Network of Sex Work Projects

Promoting Health and Human Rights

COMMUNITY guide

Digital Security

Introduction

The digital transformation of society is an ongoing phenomenon, accelerated by the growing use of information and communication technology (ICT) in the last decade. ICT refers to the internet, dating sites, escort sites, smartphone apps, social media platforms and many more. ICT is profoundly transforming how sex workers communicate, organise, socialise, and work.

ICT use amongst sex workers is rising, and a growing number of sex workers are migrating from street-based to indoor work, due to the increasing availability of the internet and online platforms as well as tools such as smartphones and tablets. Using these technologies can have many benefits for sex workers. Additionally, ICT can be a valuable tool for national and international NGOs and government service providers to reach out to sex workers and provide information, improving their access to health services, safety, and justice. However, the increased digitalisation of everyday life also poses new threats and challenges for sex workers that need to be addressed.

Key Issues

Harmful laws governing digital spaces and their impact on sex workers

Digital spaces are shrinking, and sex workers are facing additional discrimination due to harmful laws making them more vulnerable to poverty and increasing the level of threat to their well-being, both on and offline.

There is a clear link between laws enacted in the USA such as FOSTA/SESTA and their impact on the wellbeing of sex workers in other countries, as many digital services that operate globally are bound by US laws in their terms of service.

In countries with data protection laws and regulations, many sex workers expressed a complete distrust of such measures due to frequent data leaks and governments' inefficiencies. Lack of regulation leaves citizens without an option to challenge the use of their data while enabling police officers' full access to any data.

Data protection

Data can be gathered through many channels such as web pages, apps, and biometrics without the knowledge or active consent of sex workers.

Surrendering sensitive data can also be a precondition to accessing face-to-face services and online platforms. Sex workers may be asked to share their names and other personal information with service providers in order to access vital services. This data is often stored in centralised databases, with varying levels of security measures. However, the fast-changing nature of ICT and the possibility for human error when storing data can make data collection extremely dangerous.

…the increased digitalisation of everyday life also poses new threats and challenges for sex workers that need to be addressed.

Sensitive data can be acquired by individuals seeking to exploit and abuse sex workers through blackmail and threats by individuals or police officers. Sex workers frequently report police practices of targeting websites, social media platforms and dating apps to gather information on sex workers, to demand money or sex.

Services are also increasingly being encouraged to undertake online outreach, using messaging and dating apps, and to use the built-in analytics of such technology to track user activity. However, private sector tech developers have very different motivations and priorities, and service providers must be made aware of how these online platforms and applications might use or share the data collected with third parties such as advertisers, shareholders, and even governments.

Algorithmic threats

Artificial Intelligence (AI) technologies often reflect race, gender, and class-related biases and reinforce structural inequalities. Consequently, sex workers are more likely to be the subject of 'potential crime maps' and place-based predictive policing.

Additionally, the race and gender biases replicated by some algorithms used in many platforms cause predominantly female, trans people and racialised sex workers to be restricted or banned. Examples include nipple bans aimed at cis and trans women or algorithms that calculate naked skin ratio to decide whether specific content is explicit or not, in which darker skins are mismarked as 'explicit'.

The rise of biometric surveillance technologies is a matter of great concern, especially for sex workers, due to the harms caused to their privacy and safety.

Content moderation via AI on social media platforms presents a growing threat to the self-organisation and the freedom of speech of sex workers in online spaces. AI is not sensitive enough to correctly judge the context, so the use of words such as 'sex' is often flagged, resulting in banning the social media accounts of sex worker-led organisations or the removal of their content.

Good practices

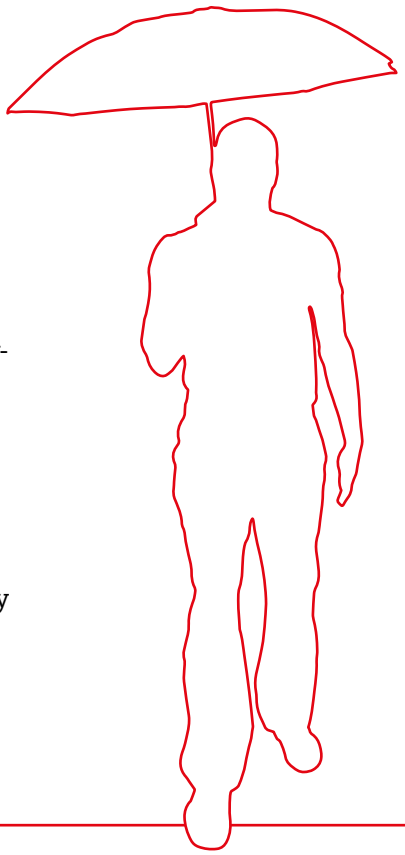
Many sex worker-led organisations are working to identify the harmful effects of digital technologies and develop valuable counter-strategies against these threats. These strategies must be updated regularly to keep track of the rapid evolution of these technologies and address the unique needs of diverse sex worker communities.

The meaningful involvement of sex workers in the development of digital services is a precondition for creating good security features addressing the unique needs of criminalised populations.

Sex workers are the experts in their lives; they should occupy leading roles in innovation. Sex workers have already initiated projects, such as online 'bad date lists' to tackle problems faced by the sex worker community. Other initiatives to tackle the censorship, online abuse, and discrimination sex workers face in traditional online platforms have also been launched by sex workers, such as Switter or Tryst. Sex worker-led initiatives showcase inclusive practices in tech while providing much needed safe spaces for the community.

When designing services for their communities, sex workers pay careful attention to data and privacy protection measures, including minimum data collection, enabling anonymous participation and safeguarding mechanisms for any data collected.

The rise of biometric surveillance technologies is a matter of great concern, especially for sex workers, due to the harms caused to their privacy and safety.



Recommendations

For Policymakers and Governments

- Governments must commit to a robust human rights-based approach rather than purely tech-based 'solutions' to complex societal issues. Where AI is utilised, this should include legislative measures to prevent human rights abuses that pose unacceptable risks to sex workers' privacy and safety.
- Develop stronger data protection laws specifically addressing the concerns of criminalised populations.
- Harmful regulatory laws and practices such as FOSTA/SESTA must be removed.
- Governments, policymakers, and advocates must actively pursue the full decriminalisation of sex work, including sex workers, clients and third parties.

For Funders

- Sex worker-led organisations should be supported to develop digital initiatives through funding for training, development and technical support.
- Understand the sensitive situation sex workers operate in and be flexible with documentation requirements when funding sex worker-led organisations and programmes.

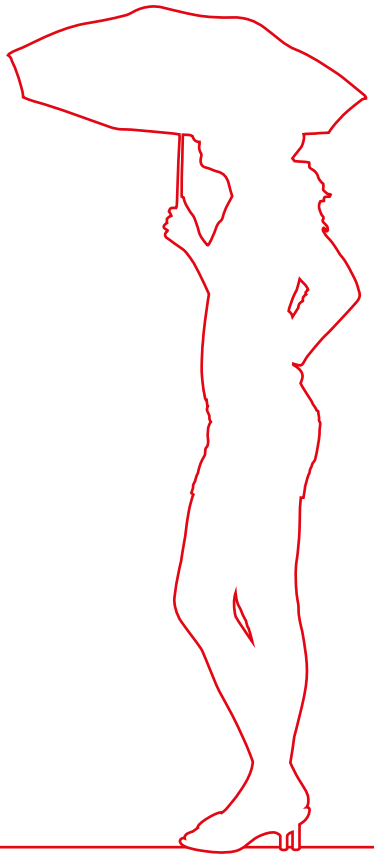
For Service Providers

- Online services should not replace face-to-face services but be used as additional tools to enhance reach.
- Identity verification should not be a pre-condition for accessing health and other services.
- Data collection should be minimised and only be used to improve the service quality. All essential data collected must be stored confidentially and securely, and only tools with strong security built-in and audited to the highest standards should be used. Ownership of the data should remain with communities – not with tech providers, and must never be shared with governments, law enforcement or other external bodies.
- The use of biometrics, data mining and harvesting, micro-targeting, geo-mapping in digital interventions with sex workers is fraught with dangers and undermines the effectiveness of service delivery. Without robust policies in place addressing the ethics and human rights concerns, they should be avoided at all costs.
- Meaningfully involve sex workers in the planning, design, delivery, monitoring and evaluation of digital services.

For Sex Worker-led Organisations

- Where possible, sex worker-led organisations should organise digital security workshops and trainings for their community and produce easy-to-access documents.

Ownership of the data should remain with communities – not with tech providers, and must never be shared with governments, law enforcement or other external bodies.



The Community Guides are the result of desk research and a global e-consultation, and aim to provide simple summaries of NSWP's Smart Guides, further detail and references can be found in the accompanying Smart Guides.

The term 'sex workers' reflects the immense diversity within the sex worker community including but not limited to: female, male and transgender sex workers; lesbian, gay and bi-sexual sex workers; male sex workers who identify as heterosexual; sex workers living with HIV and other diseases; sex workers who use drugs; young adult sex workers (between the ages of 18 and 29 years old); documented and undocumented migrant sex workers, as well as and displaced persons and refugees; sex workers living in both urban and rural areas; disabled sex workers; and sex workers who have been detained or incarcerated.

nswp
Global Network of Sex Work Projects
Promoting Health and Human Rights

The Matrix, 62 Newhaven Road
Edinburgh, Scotland, UK, EH6 5QB
+44 131 553 2555 secretariat@nswp.org www.nswp.org

NSWP is a private not-for-profit limited company. Company No. SC349355

PROJECT SUPPORTED BY:

Love Alliance
Together for health and human rights

ROBERT CARR FUND
for civil society networks