Digital Security

The Smart Sex Worker's Guide

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

nswp

Global Network of Sex Work Projects
Promoting Health and Human Rights

SEX WORK IS WORK:
Only Rights Can Stop the Wrongs

The Global Network of Sex Work Projects (NSWP) exists to uphold the voice of sex workers globally and connect regional networks advocating for the rights of female, male and transgender sex workers. It advocates for rights-based health and social services, freedom from abuse and discrimination and self-determination for sex workers.

The Global Network of Sex Work Projects uses a methodology that highlights and shares the knowledge, strategies, and experiences of sex workers and sex worker-led organisations. Smart Guides are the result of desk research and a global e-consultation with NSWP member organisations, including case studies from some members.

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.

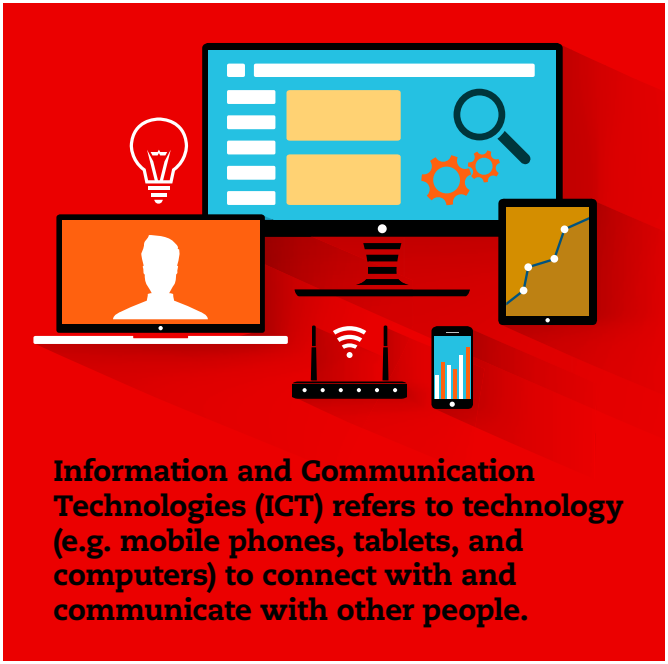
Contents

IMAGE BY MOLLY HANKINSON

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 technology (mobile phones, tablets, computers) used to connect and communicate with other people. This includes the internet, dating sites, escort sites, smartphone apps (e.g., Tinder, Grindr, WhatsApp), social media platforms (e.g., Facebook, Twitter, Instagram) and many more. ICT is profoundly transforming how sex workers communicate, organise, socialise, and work. The global race for market domination, particularly in the United States, China and the European Union, is rapidly driving the demand for innovations and the COVID-19 pandemic has significantly expanded the digitalisation of public and private spheres.

Sex workers are often among the first adopters of digital technologies to improve their safety while conducting their work in increasingly criminalised and stigmatised contexts and to protect their privacy. 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.



Information and Communication Technologies (ICT) refers to technology (e.g. mobile phones, tablets, and computers) to connect with and communicate with other people.

Using these technologies can have many benefits for sex workers, such as finding a place to advertise their services, communicating with their colleagues, screening clients, accessing key information and services, and organising politically. Additionally, ICT can be a valuable tool for national and international NGOs, as well as 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. Digital technologies, such as mobile applications and biometric surveillance practices, can also be used to find, count, identify, track, trace, and punish sex workers; simultaneously, sex workers' online safety and privacy are threatened by harmful laws that regulate online spaces, exclusionary policies of social media platforms and digital financial services. The misuse and weaponisation of artificial intelligence (AI), the ability of a computer to perform tasks that human intelligence is capable of performing, such as facial recognition technologies by governments, police forces and other law enforcement officials, and anti-trafficking organisations, present new dangers for sex workers, particularly for those whose identities intersect with other marginalised groups such as migrant, racialised and LGBT communities.

This Smart Guide identifies some of the current trends in the use of ICT, exploring good and bad practices, and examines the threats and challenges to sex workers' safety, privacy, and well-being. It highlights the need for ICT developments that meet the highest security standards, are community-led and owned, that protect the health and other human rights of sex workers, and that do not replace essential face-to-face services for sex workers or undermine community empowerment at grassroots level. The Smart Guide draws on the expertise of sex workers and key informants and concludes with recommendations for different stakeholders.

Literature review

Sex workers were amongst the first users of the internet. In an increasingly criminalised environment, they looked for safer ways to advertise for clients and connect with their communities. Sex workers were early users of online chat rooms and personal websites before they became mainstream[1]. In this sense, sex workers were the testers and quality checkers of online services and helped co-create[2] and shape the internet as we know it. Today the internet and digital technologies are an essential part of many sex workers' lives. Through digital technologies, sex workers can advertise their services, screen and communicate with clients, collect payments, connect with their colleagues and communities and find information about health and other services[3].

Additionally, the availability of online spaces allows sex workers to work in alternative settings, for example, through webcam work or subscription services, creating additional streams of income. However, the digital sphere has become an increasingly hostile environment for sex workers in recent years. Although sex workers acknowledge and express that working online is a safer way to conduct their business, a growing number of digital services are adopting anti-sex work policies seeking to deny sex workers access to their platforms while sex workers' rights to safety and privacy are threatened by intrusive practices by governments and private companies alike.

Exclusion from digital services is exacerbated and justified by repressive and discriminatory laws such as FOSTA/SESTA in the United States and others worldwide. Written under the guise of 'anti-trafficking' legislation, FOSTA/SESTA is used to curb online sex work by making online communications regarding selling and purchasing sexual services potentially illegal.[4] The bill implements an exception – in the case of online sexual activity – to the long-standing principle that platforms should not be treated as publishers of content, a central principle of the internet.

Shortly after the introduction of FOSTA/SESTA, many online services and platforms attempted to avoid liability by revising their terms and conditions to exclude sex workers[5]. In the USA and elsewhere, sex workers have lost their web pages and professional adverts on platforms.

1 Chanelle Gallant, "The Social Network Sex Workers Built," Bitch Media, 17 December 2018.

2 Sofia Barrett-Ibarria, "Sex Workers Pioneered the Early Internet—And It Screwed Them Over," VICE, 3 October 2018.

3 NSWP, 2017, "Smart Service Provider's Guide to ICT and Sex Work," p2.

4 NSWP, 2018, "U.S.A. FOSTA/SESTA legislation."

5 Jaimee Bell, "FOSTA-SESTA: Have controversial sex trafficking acts done more harm than good?," BIG THINK, 22 January 2021.

Many online spaces such as Backpage.com[6] that previously allowed sex workers to advertise and find clients in a safer environment were shut down. OnlyFans, which for many sex workers had become a vital source of income, particularly during the COVID-19 pandemic, briefly announced a ban on 'any content containing sexually-explicit conduct', after pressure from its payment processors. It later reversed the decision[7]. Online payment systems such as PayPal[8] now frequently cancel the accounts of sex workers, on some occasions even blocking access to funds held[9], based on policies that forbid transactions for "certain sexually oriented materials or services", thus contributing to the impoverishment of sex workers. Online platforms such as Facebook, Instagram, YouTube and others ban or 'shadowban' (banning a user or content in a way that is not apparent to the user) profiles of sex workers or remove their content, often without warning or providing ways to appeal the decision. As a result of this exclusion, sex workers become more isolated and are deprived of necessary services that support them to work safely. According to a community report[10] from 2020 highlighting the impact of FOSTA/SESTA on sex workers, 72.5% of participants said they were facing increased economic instability after the introduction of the law, while 33.8% reported an increase in violence from clients.

Digitalisation also brings renewed threats to sex workers' safety and privacy. For sex workers, protecting their data is of utmost importance. Especially in a criminalised context, the boundaries sex workers establish in their day-to-day lives provide the necessary protection against stigma, discrimination, and violence. For example, many sex workers prefer to have a separate online identity for work. However, algorithms and the lack of transparency regarding how they function erase sex workers' efforts to separate their work and private identities. Facebook's 'People You May Know' algorithm[11] is known to pool user information from different platforms and devices into Facebook, causing sex workers' private accounts to be visible on clients' or family members' screens, therefore removing the safety protections established by sex workers.

6 Matt Baume, "The Backpage.com Shutdown is Making Life Hell for Sex Workers," Them, 9 April 2018.

7 NSWP, 2021, "NSWP Statement: NSWP Welcomes OnlyFans' Reversal of Decision to Ban Sexually-Explicit Content."

8 Paris Martineau, "A Quiet War Rages Over Who Can Make Money Online," WIRED, 30 November 2018.

9 Catherine Barwulor et al., ""Disadvantaged in the American-dominated internet": Sex, Work, and Technology," SocArXiv Papers (2020).

10 Hacking//Hustling, 2020, "Erased—The Impact of FOSTA-SESTA and the Removal of Backpage 2020," p.17.

11 Kashmir Hill, "How Facebook Outs Sex Workers," GIZMODO, 10 November 2017.

IMAGE BY MOLLY HANKINSON

This, in turn, can cause sex workers to be outed, 'doxxed' (revealing identifying information of someone online), harassed, stalked, blackmailed or to face other abusive behaviours that put their well-being and lives in danger. Additionally, data mining/harvesting practices are common amongst social media platforms and other online services. The collected data is sold to private companies to target audiences for advertising to maximise their profits. The implications for personal safety and privacy, and more broadly for democracy, can be extremely dangerous, as illustrated by the Facebook-Cambridge Analytica scandal in 2016, when, without users' knowledge, the data of 87 million Facebook users was shared with the British consulting firm and used targeted political advertising to influence the elections in the USA.[12]

The infringement of the security of sensitive data occurs on webcamming platforms. Sex workers are increasing their use of webcamming and online modelling platforms due to the low entry requirements and lower potential risks. This has grown significantly during the COVID-19 pandemic as they look to earn money without violating social distancing rules and curfews[13]. However, non-consensual sharing of recordings of shows and capturing images (capping) occur regularly[14].

Data collection in service provision, including ICT-mediated health services, is also greatly expanding. New e-health initiatives are becoming more widely available, bringing specific advantages and disadvantages. For example, the rollout of e-health services can increase sex workers' awareness of and access to HIV and other key services and can also help fight against disinformation regarding sexual health that has become widespread in recent years, by providing centralised and accurate information.

12 Issie Lapowsky, "How Cambridge Analytica Sparked the Great Privacy Awakening," WIRED, 17 March 2019.

13 Alex J. Nelson et al., "Sex Work during the COVID-19 Pandemic," Society for the Anthropology of Work (2020).

14 Stewart Cunningham et al., "Behind the screen: Commercial sex, digital spaces and working online," Research Gate (2017), p.2.

Through these initiatives, valuable data can be collected, which could be useful to create population size estimates to adjust the service capacity, to better understand the needs of communities, and to provide data to donors to justify continued or increased funding. However, collecting sensitive data can put sex workers' privacy and safety in danger, for example, if data protection measures are insufficient and law enforcement officials are able to procure it. International guidance produced in 2013 (known as the Sex Worker Implementation Tool, or SWIT)[15], highlights the importance of data protection when mapping criminalised populations such as sex workers. The SWIT emphasises that data collection must be done in a way that considers the needs and safety of sex workers, with local sex workers and their organisations leading and shaping the process for new interventions. Mapping and population size[16] estimates should be used only to improve service provision, and extensive data collection must be limited. Mapping the venues or physical locations frequented by sex workers is extremely sensitive and potentially dangerous. If shared with local law enforcement or national government departments, the information could be misused to target locations for arrest, raids, crackdowns, harassment, and violence. Confidentiality, storage and data security are paramount concerns 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, rather than tech developers or government departments.

The risks of employing biometric technologies in service provision must be scrutinised, and sex workers must be meaningfully involved in related discussions. The involvement of sex workers should not be limited to mere consultation, nor should they be simply informed of health services aimed at them – they must be able to choose how they are represented and by whom, how they are engaged in the processes, whether to participate, and have an equal voice in how partnerships are managed.[17]

The use of biometrics in health and other service provision and in key population surveys has been opposed by sex workers around the world and can seriously impact the efficiency of the services due to mistrust within the community. Biometrics can include taking fingerprints, iris or retina scans, DNA, toe prints, and newer forms can even identify individuals through gait, voice, facial recognition, and can conduct iris scans in crowds through surveillance videos.

15 WHO, UNFPA, UNAIDS, NSWP, World Bank & UNDP, 2013, "Implementing comprehensive HIV/STI programmes with sex workers: practical approaches from collaborative interventions."

16 NSWP, 2015, "Mapping and Population Size Estimates of Sex Workers: Proceed with Extreme Caution," p.14.

17 NSWP, 2017, "Briefing Paper: The Meaningful Involvement of Sex Workers in the Development of Health Services Aimed At Them," p.3.

A case study report from Kenya[18] highlights the mistrust of the use of biometrics in health services amongst sex workers and other key populations due to the risk of possible data leaks and their consequences, especially in criminalised contexts, including biometric data potentially being used by police to target key populations for arrest. Some of the human rights concerns in the use of biometrics included "function creep, the growing and under-regulated role of private companies, and the risk of data breaches which could lead to worrying violations of privacy." Even data protection policies may not be sufficient to counteract these concerns, "if a change in leadership put new leaders in place who chose to override it, or if a court ordered a health agency to share biometric data with the police." Overall, the use of biometrics with criminalised populations such as sex workers is fraught with dangers and "could undermine the effectiveness of HIV surveillance efforts and trust in the AIDS response as a whole. Clearer policies that address the use of biometrics in HIV surveillance activities and are responsive to ethics and human rights concerns are needed for governments, research ethics boards, and funding agencies."[19]

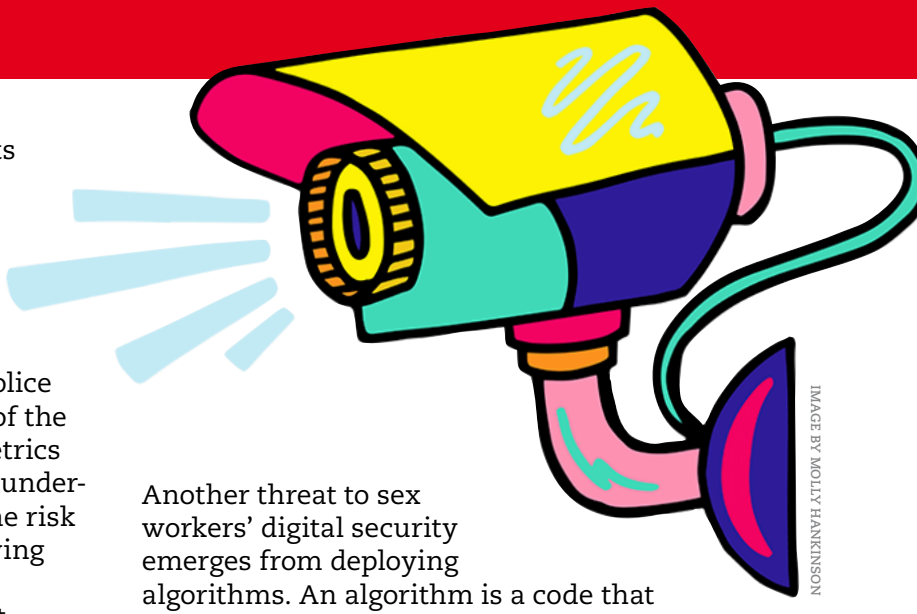


IMAGE BY MOLLY HANKINSON

Another threat to sex workers' digital security emerges from deploying algorithms. An algorithm is a code that helps a computer system complete a task, such as recognising patterns. Their use by private companies and governments is expanding, but their potential negative impacts, especially on sex workers and other marginalised populations, must not be ignored. Law enforcement can use algorithms to make predictions about future crime locations based on data from past incidents. Algorithms are also used to identify supposed 'victims of human trafficking' online by analysing the pictures and text from adverts of sex workers[20]. However, the 'indicators' purported to signal human trafficking are always based on past data collected by law enforcement and can be as vague and inconsequential as the presence of a tattoo or the way a person poses in an image, making the process and the outcome discriminatory and irrational. Due to the conflation of sex work and trafficking, algorithms replicate the discrimination embedded in current law enforcement systems and target sex workers.

18 KELIN, 2018, ""Everyone said no" Biometrics, HIV and Human Rights A Kenya Case Study."

19 Matthew M. Kavanagh, PhD et al., "Biometrics and public health surveillance in criminalised and key populations: policy, ethics, and human rights considerations," The Lancet HIV (2018).

20 Rebecca Enright, "SWOP coalition on Pitt's "Hacking for Humanity," The Tartan, 21 March 2019.

The resulting over-policing of sex workers, particularly migrant[21] and racialised sex workers, increases criminalisation, stigma, violence, loss of income, and risk of deportation.

Law enforcement and migration officials can also use algorithms to track, trace, and count sex workers through biometric mass surveillance. When deployed in public spaces, technologies like facial recognition gather large amounts of data which are stored in police databases to 'train' the algorithms. However, these practices enable "disproportionately powerful groups to further fortify their power over socially-marginalised groups such as people living in poverty or social exclusion, people of colour, or human rights activists."[22]

Additionally, this non-consensual collection and storing of sensitive personal data such as fingerprints, face, and voice violate sex workers' human rights to privacy and freedom from arbitrary interference and safety and further deepens the discrimination against migrant and racialised sex workers.

21 NSWP, 2018, "Briefing Paper: Migrant Sex Workers."

22 EDRi, 2020, "Ban Biometric Mass Surveillance," p.13.

Key findings from the NSWP consultation

NSWP carried out a global e-consultation with its member organisations and conducted in-depth interviews with key informants from several countries to gather information regarding the digital security of sex workers.

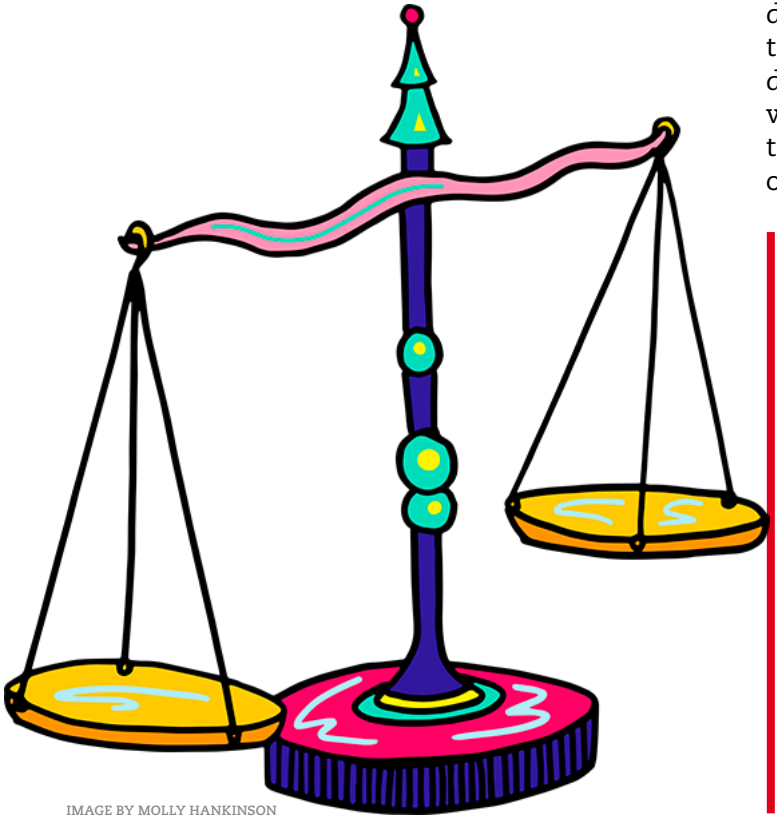


IMAGE BY MOLLY HANKINSON

1 Harmful laws governing digital spaces and their impact on privacy, safety and wellbeing of sex workers

Sex workers face additional discrimination due to national and international laws and policies that regulate digital spaces, supposedly aiming to create a 'clean' digital environment by using different exclusion methods. Many respondents talked about the shrinking of their digital spaces due to harmful laws and how these make sex workers more vulnerable to poverty and increase the level of threat to sex workers' wellbeing, both on and offline.

> ***"In French law, pimping is defined very broadly, and hosting providers for sex workers' websites or advertising platforms can face penalties. This damages sex workers' ability to work online and can result in suspended or deleted accounts, preventing sex workers from collecting their earnings. Many sex workers, therefore, need to register on foreign platforms, which can create different problems. Sex workers sometimes need to pay for intermediaries to provide them with technical support to avoid danger, so the law also increases the need for intermediaries. There are several cases of sex workers' accounts deleted, personal and for work use. Other sex workers are banned from Airbnb because their phone numbers are linked to sex work although they did not use Airbnb for sex work purposes."***
>
> MÉDECINS DU MONDE, FRANCE

> ***"There is a law against pimping, porn and other explicit content in Ukraine. So, sex workers can be charged and treated as criminals."***
>
> LEGALIFE-UKRAINE

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.

> ***"Even sex workers who live in Belgium are using the American networks that are under the rule of FOSTA/SESTA. This is reducing their ability to work and create content on sex work-related issues."***
>
> UTSOPI, BELGIUM

The exclusion from online spaces is not limited to individual sex workers. Sex worker-led organisations also frequently face bans on online platforms.

> ***"Twiggy's Facebook account has been suspended on several occasions for expressing our voice as sex workers since the historical vindication of the nudity of the trans woman's body as a political act."***
>
> TWIGGY FUNDACIÓN, COLOMBIA

In countries with data protection laws and regulations, many sex workers expressed a complete distrust of such protections due to frequently occurring data leaks and governmental inefficiency in providing solutions to problems. In some countries, a lack of regulations defining and protecting the right to privacy leaves citizens without an option to challenge the use of their data while enabling police officers' full access to any data.

> ***"Singapore does not recognise the right to privacy or have a Freedom of Information Act. A range of laws allows various state agencies intrusive access to personal data. Under the Telecommunications Act, telecommunications providers can be ordered to control telecommunications equipment and censor or stop messages. The Computer Misuse and Cybersecurity Act (CMCA) allows collecting information from any computer, including in real-time. The Criminal Procedure Code (CPC) allows police officers or appointed third parties to obtain any data that is deemed necessary without judicial authorisation."***
>
> PROJECT X, SINGAPORE

2 Data protection, censorship, organising, safety and privacy issues:

Although the amount and type of data collected may vary, any kind of data collection can threaten sex workers' privacy and security if it ends up in the wrong hands. Data can be gathered through many channels such as web pages, apps, mobile banking systems, and biometrics without the knowledge or active consent of sex workers, which constitutes unacceptable risks to sex workers' safety and privacy.

However, 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 HIV, sexual health another vital services. This data is often stored in a centralised database with varying levels of security measures. However, the fast-changing nature of ICT and the possibility for human error when storing data can make the practice of such data collection extremely dangerous, especially for criminalised populations such as sex workers.

The power of online platforms to collect data increases exponentially, especially when they enjoy a monopoly in the market. The gatekeeping power of platforms creates a forced membership system where sex workers have no choice but to register if they want to work.

Although this situation may negatively impact any sex worker, the risk is higher for sex workers who live in precarious settings such as single mothers, homeless sex workers and sex workers who use drugs, since they cannot afford to choose privacy over securing work.

> ***"It is known that moderators and administrators of advertising platforms often require sex workers who advertise on them to verify their identity. Photos with open faces, sometimes even passport data, are asked. This is done ostensibly to make sure sex workers are above the legal age. However, there are instances when this information fell into the hands of outsiders, and sex workers were blackmailed. This is often the case for webcam studio owners and intermediary managers between sex workers and clients."***
>
> SEX WORKERS FORUM, RUSSIA

Protecting sensitive data is crucial to ensure sex workers' online and offline safety. However, many sex workers experience difficulties in safeguarding their data when working online. Many members mentioned instances of sensitive data being acquired by individuals looking for ways to exploit and abuse sex workers through blackmail and threats.

> ***"The revelation of people's sex work status by others is a big threat. There is always a risk of clients finding the personal account of sex workers."***
>
> UTSOPI, BELGIUM

> ***"In Kazan, there was a case where a sex worker conducted a webcam session, and the client recorded it and began to extort money from the girl with the threat of outing her. The perpetrator also found the workers' social media profiles and made a list of her friends. The sex worker filed a complaint with the police about extortion, but the police did not investigate. On the contrary, they threatened the girl with punishment for prostitution and for violating the lockdown rules."***
>
> SEX WORKERS FORUM, RUSSIA.

When any aspect of sex work is criminalised, sex workers are especially vulnerable to blackmail and other forms of abuse as they avoid filing complaints to the authorities for fear of getting fined or arrested.[23]

> ***"There are instances of sex workers' photos or videos from cam shows are captured by individuals who then use those to blackmail them. And often, sex workers cannot go to the police because it is illegal to put explicit content online."***
>
> LEGALIFE-UKRAINE

Many respondents also reported that police target websites, social media platforms and dating apps to gather information on sex workers, to demand money or sex. This is also common in many countries when a sex worker is arrested, and the police confiscate their phone in order to acquire information about other sex workers.

> ***"Law enforcement also go through sex workers' phones when they are arrested, paying special attention to their messages and Google Translate history. This is then used to prove that they are sex workers, and they're then sentenced and/or deported."***
>
> PROJECT X, SINGAPORE

> ***"Blackmail by law enforcement to extort money from the female sex worker is a real problem. For example, when sex workers are arrested, their phones can be used to get incriminating information to blackmail and get bribes from them. This has a financially crippling effect on sex workers."***
>
> ALLIANCE OF WOMEN ADVOCATING FOR CHANGE, UGANDA

Several respondents expressed growing concern about the increased surveillance of sex workers during the COVID-19 pandemic, through social media or advertising platforms. Governments have used the COVID-19 pandemic to justify increased police surveillance, with sex workers and other marginalised communities being disproportionately targeted.

> ***"During the confinement, there was a sort of "hunt" for sex workers via the networks [Grindr]. COVID-related regulations have increased the control of the police."***
>
> UTSOPI, BELGIUM

23 NSWP, 2020, "Briefing Paper: Sex Workers' Lack of Access to Justice."

The growth in ICT-mediated health services is of particular concern. As services look for new way to increase the take-up of services, often with the encouragement of, or even under pressure from, donors and funders, ICT may seem like an easy solution. Concerningly, programmes and services are increasingly being encouraged to look towards online and mobile platforms to engage services users through online outreach, including using social media sites, messaging and dating apps. One programme implementer guide[24] advises programme staff to "contact the app developer to learn about appropriate ways to engage users" and using built-in analytics of social media platforms to "track how specific subgroups respond to different targeted messages and how frequently they act by getting tested and entering treatment". This level of tech developer joint-working with service providers, including sex worker-led organisations, is of enormous concern given private sector tech developers have very different motivations and priorities. Service providers and sex workers must be 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.

IMAGE BY MOLLY HANNINSON

24 FHI 360, LINKAGES Project, 2019, "A Vision for Going Online to Accelerate the Impact of HIV Programs," pp 18 & 23.

The collection and storing of digital data also pose threats for sex worker-led organisations, service providers and individual sex workers. A respondent in Uganda illustrated how police can prevent sex workers from self-organising and impede essential service provision by confiscating ICT equipment. It also shows that sensitive data can end up in the hands of people who wants to harm sex workers even when it is thought to be safe.

> ***"ICT provides information to the law enforcement which has led to barriers for services provision and research. For example, during our research survey to find out how COVID-19 affected the work and lives of female sex workers, our data officers' phones were confiscated by the police and used to gather information and knowledge about the research survey [which] was later stopped by the police. This led to a barrier on getting the necessary information about the needs of female sex workers, thus creating a limitation of the necessary interventions to provide the goods and services to the community."***
>
> ALLIANCE OF WOMEN ADVOCATING FOR CHANGE, UGANDA

Government surveillance of social media or escort advertisement platforms was also mentioned as a significant barrier against sex worker organising, especially in countries such as China, where sex workers and sex worker-led organisations face extremely high levels of censorship and the threat of criminalisation when organising online.

IMAGE BY MOLLY HANKINSON

> ***"It is very difficult and dangerous to organise in China. Online spaces are under constant surveillance, and the Chinese government regulates the internet very strictly. They have so much data about everyone. For example, you can get in trouble with the police for using certain words such as 'human rights' when chatting online or on dating apps. So, to be able to organise, you have to find different words. You also cannot organise a gathering with more than 30 people. Otherwise, you need permission from the police."***
>
> SEX WORKER, CHINA

3 Algorithmic threats to privacy, safety and organising:

Algorithm use in areas such as policing presents evolving risks to criminalised populations, including sex workers. NSWP's consultation revealed that AI technologies are more commonly used in some countries than in others, and in countries with high prevalence of AI use, the details of the use and the impact are not always clear.

Many respondents noted that data collection by mass surveillance technologies had increased exponentially in recent years, and AI is increasingly deployed in public spaces and service provision.

> ***"Biometric data such as fingerprints and iris scans are used in passports and at borders, which is troubling when sex workers are prohibited migrants. Singapore is also increasingly using biometric data (especially facial verification and recognition) in accessing public services, such as banking and financial services, taxes, and public housing applications. Since the pandemic, public temperature scanning technology has also been implemented in public spaces, and this sometimes also uses facial recognition technology. The impact on sex workers is currently hard to measure, as these initiatives are still being rolled out. However, it is reasonable to anticipate that this will make sex work more difficult and precarious in future."***
>
> PROJECT X, SINGAPORE

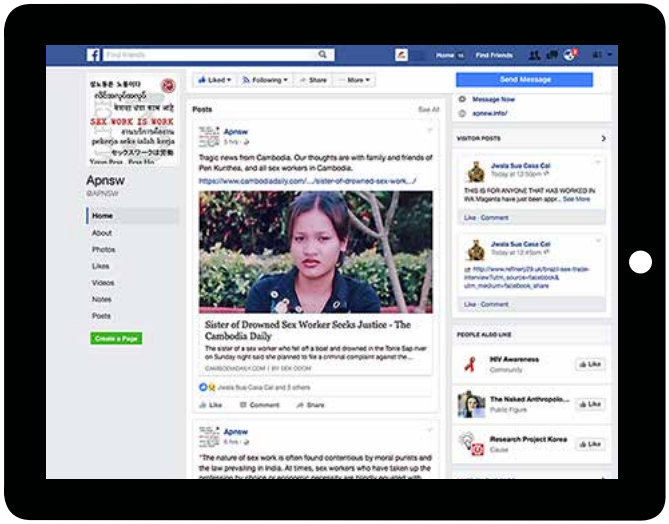
> ***"Biometric surveillance is applied everywhere in China. There are CCTV cameras everywhere. Police are using AI to surveill and punish communities, for example, sex workers and people who use drugs. Once a person is arrested, they are in the police system for good. As a result of too much surveillance, the crime rates have gone down, but it is very dangerous to live here for sex workers."***
>
> SEX WORKER, CHINA

The 'training' data used in AI technologies often reflect race, gender, and class biases and can reinforce structural inequalities. There is a heightened risk of increasing over-policing of criminalised populations. Sex workers, racialised individuals and migrants, are more likely to be the subject of 'potential crime maps' and place-based predictive policing.

> ***"The use of biometric mass surveillance is being implemented in our country and laws have been approved with the exceptional circumstances of the COVID-19 pandemic, now there are cameras and all these tools to monitor, but …due to our work, these tools hit us directly [particularly] the migrant population informal workers and sex workers."***
>
> ASOCIACION HTS GOOVER

> ***"Biometrics are used against sex workers, in particular, migrants. Recruiting companies use a person's online content through facial recognition software to ensure that the person is not a sex worker. Biometric data is used by GAFAM [Google, Apple, Facebook, Amazon, Microsoft] and the EU border police (FRONTEX) to prosecute "illegal migrants". As a result, migrant sex workers find themselves in more vulnerable situations because of these technologies."***
>
> UTSOPI, BELGIUM

Content moderation via AI on social media platforms, such as Facebook and Instagram, presents growing threats to the self-organisation and the freedom of speech of sex workers in online spaces. For example, since AI is not sensitive enough to correctly judge the context, the use of particular 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. Laws aimed at tackling online hate speech and harassment of criminalised and marginalised populations have led to the flagging of insults such as 'whore', 'putas', 'pute', terms which have been reclaimed by sex worker communities. Many sex workers stressed that access to online spaces is crucial for online organising; therefore, the systematic exclusion of sex workers from online spaces directly impacts sex workers' ability to organise and fight for their rights. Additionally, the race and gender biases replicated by some algorithms cause predominantly female, trans people and racialised sex workers to be restricted or banned.



© APNSW

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'.

Sex workers reported other discriminatory and harmful uses of AI including Airbnb using software to identify and exclude sex workers through their phone numbers, and private companies and governments using AI-powered recruitment tools to ensure the applicant is not a sex worker.

4 Good practices:

Enabling access to information, community support and peer to peer education on digital security

Sex workers and service providers acknowledge the many benefits of new technologies and the improvements they may provide in their work or private lives while pointing out new risks and challenges stemming from the accelerated digitalisation. As mentioned by NSWP member organisation Faith, Hope, Love in Ukraine *"on the one hand, for our organisation, the use of digital technologies is good, as it allows us to increase the coverage of our services, but on the other hand, if the police use them, it increases the risk of reprisals against women."* However, ICT has become an essential part of sex workers' lives, enabling the creation of new strategies and tools to tackle issues they face.

> ***"We have collectively embraced ways to protect ourselves and be in permanent dialogue with each other by using, for example, Grindr, Facebook, Twitter, thus creating alerts in the event of any danger, this has given positive changes that have benefited us. Also, a prevention issue in sexual and reproductive health has been achieved by creating strategies such as cybersex and also despite the confinement, we have been able to be in permanent dialogue so that our work is not lost or we regress in rights before policies and governments that criminalise our work practice."***
>
> ASOCIACION HTS GOOVER

Sex workers and sex worker-led organisations have an essential role in enabling community learning and enhancing digital literacy among sex workers. This learning exchange plays a vital role in minimising risk, as sex workers know their needs best and how to meet them. Many sex worker-led organisations are working to identify the harmful effects of digital technologies and develop valuable counter-strategies against these threats. There are increasingly more resources and training produced by sex workers and sex worker-led organisations focusing on mitigating the risks of digital technologies while still benefiting from what they can offer.

> ***"The Sex Workers Forum, in its internet resources and in the new 'Take Care of Your Online Safety' brochure for sex workers, describes the risks of digital privacy violations and advise on how to avoid them."***
>
> SEX WORKERS FORUM, RUSSIA

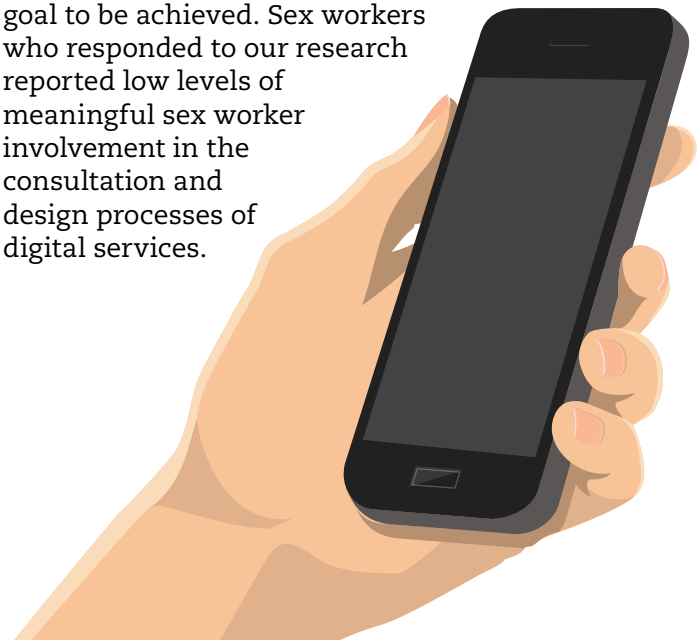
> ***"In Ukraine, through the use of ICT, we distribute information on various topics such as police activities. We also distribute awareness-raising materials about how to do webcam shows safely and other tips for working online safely."***
>
> LEGALIFE-UKRAINE

Some digital security practices sex workers adopt include VPN (virtual private network) use, having separate phones and SIM cards for work and private life, password protection, using encryption, and choosing browsers, platforms, email providers, apps and other communication tools that offer better data protection and privacy options. While many of these strategies can enhance security, many respondents noted that they should not be seen as solutions to all the risks digital services may create. While digital harm reduction and protection strategies are useful for many sex workers, these strategies must be updated regularly to keep track of the rapidly evolving aspects of these technologies. When developing procedures and good practices to ensure digital security, the unique needs of diverse sex worker communities need to be taken into consideration. For example, street-based sex workers may have different needs compared to indoor workers and others. Similarly, migrant and racialised sex workers should be consulted to identify and address their specific problems and contextual needs.

> ***"All good practices depend on the context. We must first understand the needs of communities before we can develop strategies. Once we know the problems, then we can organise digital security training and produce localised resources."***
>
> DIGITAL DEFENDERS PARTNERSHIP

Meaningful involvement of sex workers in the design of digital services

There is a clear trend towards ICT use in service provision globally. However, the meaningful involvement of sex workers and other key populations in the planning, design, delivery, monitoring and evaluation of digital services has not yet been extensively achieved. The traditional approach to innovation that sees users as passive recipients of goods and services is still the mainstream approach worldwide. It is crucial to understand the importance of the early inclusion of sex workers in the innovation process and co-development of technologies to establish ethical innovation practices and trust. Moreover, sex worker leadership and community-led service design should be acknowledged as a goal to be achieved. Sex workers who responded to our research reported low levels of meaningful sex worker involvement in the consultation and design processes of digital services.



However, some members mentioned a change in this situation.

> ***"We have participated in a passive role, that is, as users, most of the time they have not given talks and workshops on the use of ICT and their security as well as some other research. But in more recent years we have been taken into account more. Through consultations, case studies and talks on issues of access and barriers in technologies, where we exercise a more leading role, and we hope it will continue like this since we think that our participation should no longer be from a spectator position. We must be included in the development, implementation and execution of all these new dynamics."***
>
> ASOCIACION HTS GOOVER

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 and marginalised populations and builds a user base through establishing trust. Digital services made with low levels of engagement with users will fail to provide benefits to key populations.

Nevertheless, best practices in some countries do showcase what good innovation practice looks like when creating digital service provision tools. For example, the Jasmine Project in France demonstrates how sex workers can and should be engaged and included in innovation from the beginning.

The Jasmine Project is an online tool that aims to establish a holistic approach to service provision for sex workers by providing helpful information and resources about different aspects of sex work in France, including law, health and wellbeing, legal and social support. They also disseminate information on dangerous clients, with a rating that indicates the level of danger, and this can be accessed through the website or the Jasmine app for mobile devices. The service, used by more than 9,000 sex workers, established high levels of approval and trust of the sex worker community in France for several reasons. Firstly, sex workers have been closely involved in every stage of service development from the start.

> ***"Jasmine app was developed after a two-year consultation process with sex workers to understand the digital needs of different sex worker groups. Every message and section of the app was discussed and designed together with sex workers. That is why it is used widely, trusted and well-liked."***
>
> JASMINE PROJECT, FRANCE

Jasmine Project also took into consideration the unique needs of a diverse range of sex workers. The app and the information on the website are available in 10 languages to maximise their reach to migrant sex workers. Translation was also coordinated with sex workers and sex worker-led organisations where possible.

> ***"The Sex Workers Forum was directly involved in the work of the French project Jasmine. One of the participants of the Sex Workers Forum is translating the data from French into Russian. Another member of the Forum disseminates information about this resource among sex workers who travel to work in France and gives them access to the list of dangerous clients through their account."***
>
> SEX WORKERS FORUM, RUSSIA

New users must be vetted by a sex worker-led group or current users to be included in the project. This is to keep the service a safe space for sex workers. Additionally, sex workers can register with a nickname without providing documentation of any kind. The data collected from users is kept to an absolute minimum to enhance the privacy and security of sex workers. The database is protected by staff members who have exclusive access to any data.

Despite the success of projects such as the Jasmine Project, barriers to their sustainability remain. Funding is often scarce for sex worker-led projects that meaningfully involve sex workers and recognise their rights, especially in countries where any aspect of sex work is criminalised. Additionally, the terms and conditions for registering new apps in app stores are increasingly restricted due to harmful laws governing online spaces.

> ***"[The] abolitionist context makes it very hard to campaign for sex workers' rights due to censorship and criminalisation. It also makes it hard for service provision. Funding is needed for us to be able to provide our much-needed services."***
>
> JASMINE PROJECT, FRANCE

Sex worker-led initiatives and innovations

Another example of good practice in ensuring the digital security of sex workers is to recognise sex workers' agency and enable sex workers' inclusion in leadership positions within digital service provision and innovation. Sex workers are the experts in their lives; they should occupy leading roles in innovation processes. Sex workers worldwide have already initiated some projects, such as online 'bad date lists' to tackle problems faced by the sex worker community.

> ***"Sex workers in Russia welcomed the creation and management of the list of dangerous clients in regions and cities. They play an active part in creating and disseminating information, including the Sex Workers Forum's resources."***
>
> SEX WORKERS FORUM, RUSSIA

Other initiatives that aim to tackle the censorship, online abuse, and discrimination sex workers face in traditional online platforms have also been launched by sex workers in recent years, such as Switter or Tryst. These initiatives are increasingly valuable due to growing hostility towards sex workers' presence on many other platforms. Sex worker-led initiatives can showcase inclusive practices in tech while providing much needed safe spaces for the community. However, the reach and accessibility of such platforms are still limited to high-income countries due to lack of funding, limited digital literacy and censorship.

The creation of sex worker-led initiatives does not necessarily remove sex workers' need to use traditional platforms such as Facebook, Twitter, and Instagram, as well as sex worker advertisement platforms where they can reach higher numbers of clients, as many of the sex worker-led initiatives are not yet widely known.

> ***"Switter, Tryst, and the other projects by Assembly 4 have been well-received in certain contexts, to my understanding. However, they're not commonly used in Singapore. There is an imbalance, globally, in where sex-worker led/centred projects spring up, and this is even truer for tech-related/digital security projects."***
>
> PROJECT X, SINGAPORE

When designing services for their communities, sex workers pay great attention to data and privacy protection measures, including minimum data collection, enabling anonymous participation, and safeguarding mechanisms for any data collected. However, some donor reporting requirements still present barriers against data protection.

> ***"When providing services, we try to collect as little data as possible. We used to collect more data, such as real names on an attendance list which was a requirement from our donors. But then we negotiated with our donors and explained to them that there could be problems with collecting that kind of data. Now sex workers can provide just a pseudonym, and we inform them that any data they provide is strictly confidential."***
>
> LEGALIFE-UKRAINE

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. All AI use should be subject to transparent regulatory human rights review before being deployed, including consultation with sex workers and sex worker-led organisations.
- Develop stronger data protection laws specifically addressing the concerns of criminalised and marginalised populations. Firewalls and other data security practices must be widely adopted for public authorities engaging with criminalised and marginalised 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. The digital divide must be taken into consideration when adopting digital service provision
- 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, etc. in digital interventions with sex workers is fraught with danger 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 to enable peer learning processes.

Conclusion

Although ICT and digital services offer many benefits, sex workers face exclusion from digital platforms and services, often exacerbated by the harmful laws criminalising sex work that contribute to their increased risk of violence, discrimination, isolation, economic insecurity and poor health outcomes, including HIV. The increase in data collection by online and offline services, government and private actors brings additional risks of data infringements that threaten sex workers' rights to privacy and safety.

While ICT-mediated health services can create new opportunities for engagement with sex workers, the potential of eroding vital face-to-face services can reduce the comprehensiveness of services while excluding sex workers who do not have access to these technologies. Extensive data collection in service provision can also lead to data protection infringements, putting sex workers at risk of increased surveillance and law enforcement, and harms the establishment of trust between sex workers and service providers.

The use of AI in online and offline spaces can have harmful effects on sex workers and other marginalised populations due to inherent bias and their weaponisation by law and border officials. Biometric mass surveillance is especially detrimental for criminalised populations who often rely on privacy to stay safe and is not compatible with fundamental human rights.

Sex workers and other criminalised populations must be included in the decision-making and design processes of digital services and technologies. Adopting a co-creation and ethical approach can radically decrease the potential of human rights violations and other risks stemming from bad design practices, while establishing trust between users and digital services and technologies. Very best practice would see the delivery and ownership of such services by the communities themselves.

While many threats posed by digital technologies can be due to faulty hardware or software, poor planning and design, or biased algorithms, all the risks are heightened by the criminalisation of sex work. The criminalisation of any aspect of sex work renders sex workers more vulnerable to human rights violations and poor health outcomes. Sex work must be decriminalised to enable sex workers' access to key services and protect, fulfil and respect their human rights.

IMAGE BY MOLLY HANNINSON

nswp

Global Network of Sex Work Projects
Promoting Health and Human Rights

SOLIDARITY IN ACTION

Even before the HIV epidemic, sex workers were organising themselves. NSWP, as a global network of sex worker-led organisatons, has strong regional and national networks across five regions: Africa; Asia-Pacific; Europe (including Eastern Europe and Central Asia); Latin America; and North America and the Caribbean.

NSWP has a global Secretariat in Scotland, UK, with staff to carry out a programme of advocacy, capacity building and communications. Its members are local, national or regional sex worker-led organisations and networks committed to amplifying the voices of sex workers.

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

Love Alliance
Together for health and human rights

ROBERT CARR FUND
for civil society networks