"It's stressful having all these phones": Investigating Sex Workers' Safety Goals, Risks, and Practices Online

Allison McDonald
University of Michigan

Catherine Barwulor
Clemson University

Michelle L. Mazurek
University of Maryland

Florian Schaub
University of Michigan

Elissa M. Redmiles
Max Planck Institute for Software Systems

Abstract

We investigate how a population of end-users with especially salient security and privacy risks — sex workers — conceptualizes and manages their digital safety. The commercial sex industry is increasingly Internet-mediated. As such, sex workers are facing new challenges in protecting their digital privacy and security and avoiding serious consequences such as stalking, blackmail, and social exclusion. Through interviews (n=29) and a survey (n=65) with sex workers in European countries where sex work is legal and regulated, we find that sex workers have well-defined safety goals and clear awareness of the risks to their safety: clients, deficient legal protections, and hostile digital platforms. In response to these risks, our participants developed complex strategies for protecting their safety, but use few tools specifically designed for security and privacy. Our results suggest that if even high-risk users with clear risk conceptions view existing tools as insufficiently effective to merit the cost of use, these tools are not actually addressing their real security needs. Our findings underscore the importance of more holistic design of security tools to address both online and offline axes of safety.

1 Introduction

In recent years, there has been a massive increase in the number of sex workers working partly or exclusively through the Internet [15]. Sex work is prohibited or heavily regulated in most countries, resulting in many sex workers needing to manage digital and physical risks carefully while carrying out their work. Even in countries where sex work is legal, the profession is heavily stigmatized [63], and working legally may not be an option for all workers [59, 69]. Furthermore, sex work can be a risky business: in person, sex workers may face aggressive or violent clients, and police or immigration action [37, 59]; online, sex workers may face doxxing, harassment, or having their content stolen or misused [38]. Much like other end-users — but unlike previously studied at-risk occupations such as journalists [50] — sex workers rarely receive specialized digital security and privacy training or customized security tools.

Further, sex workers make up a sizable portion of the population: an estimated 42 million people are engaged in sex work worldwide [43, 56], spanning all genders, ethnicities, and socioeconomic backgrounds [35, 54, 64]. A growing body of sociological and HCI research has looked at how the Internet has impacted the working conditions of sex workers, including how they find and interact with clients [7, 11], conduct their businesses [63, 64], and even the forms of sex work they do (for example, supplementing in-person sex work with camming: live performance of sex acts on camera) [15, 39, 65]. Yet, while many recent studies on digitally-mediated sex work touch upon safety management [63, 64], none, to our knowledge, center the digital safety experiences and technical needs of this high-risk population.

Our research goal is to elucidate how sex workers manage their digital privacy and security. By understanding how a population that knowingly operates in risky physical, legal, and social contexts makes decisions around digital privacy and security, where the consequences of unwanted exposure can be significant, we hope to better understand (1) how technology can better address the specific safety needs of this particular population, (2) how awareness of serious risk influences digital security and privacy behavior, and (3) whether existing safety strategies and tools leave some needs unmet or force unwanted trade-offs. A better understanding of how this population manages digital safety can also inform our approach to improving digital security for end-users more broadly.

Through 29 semi-structured interviews with sex workers in Germany and Switzerland and a survey of 65 sex workers in Germany, Switzerland, and the UK (all countries in which sex work is legal but regulated), we explore sex workers' self-defined safety goals, the risks they identify to those goals in terms of both adversaries they frequently defend against as well as the digital tools that make protecting themselves difficult, and the concrete strategies and tools they use to protect themselves against those risks.

Safety for our participants encompasses multiple axes, including physical safety, financial security, having and enforcing clear boundaries, respect, privacy, legality, and access to a community of sex workers. Each of these axes of safety is dependent on others; a threat to one axis may increase the risks from another. For example, a sex worker failing to keep their legal name private may increase chances of physical threats like stalking or blackmail.

Our participants describe complex safety strategies, such as the use of multiple devices, self-censorship online, and the creation of support communities, e.g., to warn each other about dangerous clients. Yet, despite being aware of risks, and despite the serious consequences of failing to protect themselves, few participants engage with traditional tools specifically designed for privacy and security such as privacy settings, Tor, encrypted chat platforms, and password managers. Sex workers view these tools as lacking sufficient efficacy to address their risks or merit the effort of use. Instead, our work suggests the need for a more comprehensive re-imagining of what it means to be safe online, beyond individual tools and settings, including scaling the home-grown protections that high-risk users such as sex workers develop for themselves out of necessity, such as multiple identities, and protections that address both online and offline axes.

2 Related Work

Digitally-mediated sex work. Sex work is defined as the exchange of sexual services for money, encompassing a broad range of services such as escorting (i.e., full-service sex work), erotic massage, porn acting, camming (performing live sex acts on video), phone sex, professional domination (performing the dominant role in a BDSM relationship), and erotic dancing. Sex work is increasingly digitally-mediated, offering both new opportunities and challenges [37].

Prior work has examined the impact of the Internet on sex work through an economic lens. In 2011, Cunningham and Kendall found that the rise in digital sex work was due to overall increases in the commercial sex market and not from the migration of street-based sex workers to digital spaces [15]. Sanders et al. also found that, in 2016, 35% of escorts based in the U.K. were doing some form of digital sex work in addition to outdoor sex work [63]. Workers engaging in digitally-mediated sex work also had higher earnings than outdoor (street) workers [15]. Prior work suggests these economic gains are related to the Internet's utility as a tool for advertising to clients, allowing sex workers a greater amount of control over their ads and the clients they accept [7, 11, 64]. The Internet has also enabled new forms of sex work that are entirely digital, like camming [39]. Furthermore, the increased prevalence of the Internet has created new spaces for digital activism and community among sex workers [22].

The Internet can also reduce sex workers' risks. Strohmayer et al. describe the ways that sex-worker support services use digital technologies to better provide services [68], and in subsequent work examined in particular the *Bad Client and Aggressor List* used by sex workers in Canada to share warnings about potentially dangerous clients with one another [67]. Additional work shows that digital mediation of sex work reduces rates of law enforcement interactions, in turn lowering the risk of harassment or arrest [11, 15].

Nonetheless, sex workers still experience risks online and offline, and the Internet is increasingly intertwined with their safety management strategies. Several studies have discussed how sex workers manage risk via the Internet. Moorman and Harrison examine Backpage ads to learn how sex workers in the U.S. manage risk through carefully crafted ad language, and find that risk management differs across race and gender, with Black women and transgender sex workers exhibiting the most risk management [54]. Sanders et al. find in their survey of U.K.-based sex workers that most (80%) had been recent victims of crime, and enumerate ways they manage risk through strategies like using pseudonyms on digital platforms, screening for bad clients in forums, and relying on social media to have safety check-ins with friends or partners [64]. In this work, we build on existing knowledge of sex work risk management to hone in on the relationship between safety goals and risk management strategies, focusing on where digital safety strategies succeed and fail.

Digital privacy & security. There is an extensive body of research on tools and strategies for digital privacy and security. Multiple studies have examined the usability of various security tools and privacy enhancing technologies like encrypted chat (e.g., [1, 2]), Tor (e.g., [25, 72]), passwords and password managers (e.g., [9, 34]), and two-factor authentication (e.g., [14, 21]). General themes from these studies suggest that managing complex systems (as privacy and security tools often are) is difficult for many users, and the trade-offs users make based on perceived costs and perceived risks may lead to low adoption of even well-designed tools [8, 31, 62]. In this work, we examine whether users who perceive their digital risks more concretely, and who have arguably more severe risks, utilize more or different tools and protective behaviors.

Other work has focused specifically on how marginalized or otherwise high-risk populations manage privacy and security. Lerner et al. found that among transgender people, the Internet provided significant benefits in terms of activism and promoting representation of trans people, while creating new risks like blackmail and doxxing [42]. Guberek et al. studied privacy and security behaviors of undocumented immigrants, finding that participants took few concrete steps to protect their digital privacy and security [27], while Simko et al. examined U.S. refugees' digital privacy and security, finding that cultural differences impacted knowledge of digital risks, as well as the usability of security mechanisms like account recovery questions [66]. In prior work examining a high-risk occupation that depends on the Internet, McGregor et al. stud-

ied journalists' digital protective strategies and found that participants stopped using or were unable to use some secure tools because they were disruptive to or incompatible with their journalistic workflow, and that using secure tools with sources was challenging because both parties needed to use the tool for it to be effective [50]. Building on this prior work, we examine a high-risk population whose members frequently have multiple, intersecting high-risk identities, including gender identity [35] and immigration status [69]. Like journalists, sex workers often use the Internet for work, but without the specialized training or tools journalists often have.

Additional prior work has examined how technology is used in relationships with intimate partner violence (IPV) to create harm [24, 30, 46], while yet other work has examined end-users' security and privacy considerations during online dating [13, 26]. Our work focuses on digital security and privacy within commercial, regulated sexual contexts rather than non-commercial relationship contexts, though some risks may overlap.

3 Methods

We seek to understand (1) sex workers' safety goals; (2) the privacy and security challenges sex workers face in achieving those goals; and (3) the strategies workers use to mitigate those risks and achieve their safety goals. To answer our research questions, we conducted, in late 2018 and early 2019, interviews (n=29) and surveys (n=65) with sex workers in European countries in which sex work is legal.

Ethical considerations. As our participants are members of a high-risk population, we not only consulted with an ethics review board but also hired a sex worker to review our study materials for ethics and appropriateness. Further, we took care to protect participant privacy and ensure, as much as possible, that our work does not risk identifying participants. Specifically, we (1) collect no personally identifiable information, including collecting no demographic data, and (2) use end-to-end encrypted tools in all study communications. As we did not collect participants' demographics, we use gender-neutral pronouns for all participants throughout the paper.

3.1 Participant Recruitment

Our recruitment strategy was designed to capture a broad range of sex workers and their experiences, within legal, regulated contexts. We recruited interview participants by distributing recruitment flyers, both in English and German, at brothels in multiple cities, at multiple points of time, in Germany and Switzerland. We further contacted brothels and sex work organizations via email and phone calls. Organizations that were willing distributed our advertising materials to their constituents. Lastly, participants were recruited through snowball sampling, where participants recommended other sex workers. Participants were incentivized with an additional 10 Euro/CHF for referrals. Hard-to-reach populations like sex workers are often studied via such participant-driven sampling [4, 36, 51]. However, such sampling methods can limit generalizability. We used our multi-method recruitment approach to maximize generalizability — fewer than 10% of our participants came from snowball sampling.

Participants signed up for the study via an online form. They were given the option of creating an anonymous ProtonMail account for scheduling and for compensation, or providing an email address of their choosing. Overall, the recruitment process for this study took over four months; our experience collecting data is described in more detail in [60].

Participant descriptives. While we did not collect demographic information to ensure the anonymity and establish trust with our participants, many participants mentioned aspects of their identity during conversation. We can therefore describe at a high level the plurality of identities that our participants held, which shows that our sample, much like the sex worker population in Eupope [69], is diverse across many identities. Our sample contained sex workers who identify as both men and women, and not all of our participants identify as cisgender. Our sample contained participants that are immigrants from Eastern Europe, North America, and Africa, and participants who had varying levels of work authorization. Not all participants were white. Finally, the sex workers we spoke to varied in age and work experience; some had just begun working in the last year, while others had been working for multiple decades.

3.2 Interview Data Collection

Interview protocol. In our interviews, we sought to understand the safety goals, risks, and protective behaviors of our participants. Participants were first asked background questions to understand the type of sex work the participant performed and how they typically used the Internet in their work and personal life. Next, we probed their experiences of safety, asking questions such as "What is safety to you as a sex worker? How do you define safety?" We then probed their perceived risks (e.g., whether they have had a negative experience online, what types of attacks and attackers they aim to protect themselves against). We then explored participants' strategies for maintaining their online safety (e.g., "Would you say you do anything in particular to maintain your safety online?"), including probing specific behaviors such as use of security and privacy settings. Lastly, we asked participants questions about additional sex-work-related topics, outside the scope of this research paper.

Interview procedure. Participants chose to be interviewed either via chat, voice, or video. As such, there are quotes that

may contain text-speak or emojis. Based on each participant's language preference, interviews were conducted in English or German by members of the research team fluent in that language. Interviews lasted on average 60 minutes, ranging from approximately 30 minutes to 2 hours. For participant safety, all interviews were conducted using private paid "rooms" on Appear.in,[1] an end-to-end encrypted communication service. Participants were paid the equivalent of $75USD (75CHF or 60 Euros) in the form of an Amazon gift card or money transfer.[2] Following each interview session, audio recordings of the interviews, if applicable, were transcribed in the native language. German transcripts (both chat and audio) were then translated into English for analysis; bilingual members of the research team consulted the original German transcripts during analysis to ensure that tone, turns of phrase, and cultural contexts were captured and included in quotes and coding.

3.3 Survey Data Collection

After conducting interviews, we developed a survey instrument to gain a larger sample size and quantification of the same topics and emergent themes explored in our interviews. Specifically, we used an open-response question to probe respondents' definitions of safety: "How do you define safety as a sex worker? What does it mean for you to be safe?" Four closed-response questions asked about respondents' use of different digital tools (e.g., encrypted messaging applications, Tor); their use of safety strategies mentioned by interview participants (e.g., "I only communicate with clients on certain devices, SIM cards, or apps"); and how legalization of sex work and immigration status affected respondents' feelings of safety.[3] Survey participants were recruited from sex workers who contacted us to participate in the interview after interviews had concluded (early 2019), and were compensated 10EUR for roughly a 10-minute survey. As in our interview study, respondents could take the survey in either German or English.

3.4 Analysis

Interviews were analyzed using an open-coding process. Three co-authors randomly selected four interview transcripts to identify emerging themes and create a thematic framework for the interview data. After creating a codebook, two of the co-authors independently coded 10 interviews to reach clearer insights into the interview data. All interview transcripts were then double-coded, codings were reviewed by the researchers after every two to three interviews, and any disagreements were reconciled. Because the interviewers reviewed every independently-coded transcript together, we do not present inter-rater reliability [49, 53].

Responses to the open-response survey question about safety definitions were similarly analyzed using the same codebook. The results of our closed-response survey questions are reported descriptively. As this work is exploratory in nature, we had no hypotheses and thus make no statistical comparisons.

3.5 Limitations

Our results may be limited in their generalizability and by participants' willingness to share sensitive experiences. While we did our best to use many recruitment methods, conduct our study in multiple languages and at different sites, use non-judgmental language, and offer participants a high degree of privacy to encourage sharing, we cannot be sure that we exhaustively captured all possible experiences and strategies of sex workers in countries where sex work is legal. However, our results provide a set of concrete insights into the experiences and safety strategies of a high-risk population, not previously studied in the security literature.

4 Results

Based on the responses from both interview and survey participants,[4] we describe the privacy and security goals of our participants, the threats they see to those goals, and the strategies they use to protect themselves.

4.1 Definitions of Safety

We identify seven common safety goals. Most participants mentioned *physical safety*, and many talked about *financial security*, *clear boundaries*, and *privacy*. For some *respect*, *legality*, and *access to community* were important safety aspects. The ways that our participants define safety are intimately connected with their digital security needs and guide their protective strategies. By considering our participants' holistic safety goals [61], we can better understand their decision-making processes and unmet safety and security needs. While we describe each safety goal separately, these goals are interconnected and were often discussed together by participants. For example, both financial security and privacy may be necessary to minimize the risk of physical harm.

Physical safety. Most participants' definitions of safety included physical safety, which often encompassed being protected from physical assault or threat of assault by aggressive clients. As one survey participant stated, safety means *"being able to work without fear of abuse or aggression"* (S36).

[1] Appear.in recently changed its name to Whereby.com.

[2] Sex workers in Germany and Switzerland earn between 50 and 600 Euros per hour; thus we aimed to compensate them appropriately for their time participating in our study.

[3] The interview protocol, survey questions, and codebook can be found at https://osf.io/9mj7k/.

[4] We use participant IDs to refer to interview (P) and survey (S) participants.

That said, not all participants feared for their physical safety. Although we cannot report safety fears by gender due to participant protections, one participant's response suggested that their race and gender impacted their sense of safety: *"Since I am a very privileged white cis male I don't think about safety so much."* (S12) This difference in safety concerns across race and gender is consistent with other studies [54].

Many participants discussed physical safety as being related to having the necessary resources — including supplies, a safe physical space in which to work, and access to healthcare and the ability to enforce safe sex practices such as the use of condoms — to safely do their work. P11 describes:

> "Safety for me means: I can do my job in an environment that doesn't endanger me and provides me with the necessary stuff to protect me. I need gloves and condoms, for example. I also like to not be raped and killed on the job, so I prefer working in a studio with colleagues present." (P11)

Some participants described safety as when their protective strategies — including digital strategies — were in place (we discuss protective strategies in more detail in Section 4.3). For example, one participant shared:

> "I'm safe when people know where I am. . . I like when the clients send me photos before of them because when I don't know the face of the guy I am very scared." (P10)

Financial security. For many participants, financial security is a primary component of safety. Participants mentioned that financial security depends on sex workers being compensated fairly and having access to health insurance and other government and social safety nets. Financial security also ties closely into physical safety. For example, several participants mentioned that when they are financially secure, they are able to turn away clients who make them feel unsafe. For example, S31 explains:

> "I don't use drugs, don't gamble, have no debts, no financially needy relatives etc so I feel zero pressure to accept bookings. . . if I had to accept jobs against my better judgement eg someone who's obviously drunk or aggressive... or demanding services I don't offer, I would be unsafe." (S31)

Clear boundaries. Many participants' definitions of safety involved ideas of boundaries, psychological well-being, and, as S9 put it, *"to have control."* Participants reported feeling safe when their physical and sexual boundaries were respected, but also when their personal time was respected, as well as when digital boundaries they established between their work and personal lives were honored. P8 describes:

> "Safety is knowing. . . that my boundaries won't get crossed, like pushed to have unprotected sex. That I'll get paid for what I asked and that the hours will be clear and done." (P8)

Respect. Many participants connected their safety and well-being to being respected by clients and society at large. S10 stated that safety means *"not feeling that society thinks it's normal for me to get hurt."* P20 expands on this idea, saying that safety is intertwined with being protected from discrimination and stigma:

> "The absence of fear of suffering personal or financial disadvantages due to one's activity. . . where the rule of law prevails over personal reservations. Working as a [sex worker] should be recognized as a normal job." (P20)

Privacy. Respect and privacy are often linked. P6 says:

> "Privacy is directly tied in with safety from harassment these days. Safety is about working safe in a society that treats me with respect and respects my privacy as well." (P6)

For others, feeling safe is directly connected to their ability to control the privacy of their personal information from clients and/or from their social networks.

> "For me, privacy is when clients don't know my name or address and can only contact me when I allow it. . . . An unannounced visit from a friend would be something nice. An unannounced visit from a client would be a catastrophe." (P14)

Many participants worried about being "outed," or publicly identified as a sex worker against their wishes. The potential consequences of being outed range from embarrassment to blackmail and threats of physical violence. P10 shared:

> "I have a friend who [was blackmailed]. And if she didn't pay [the blackmailer], [they] would tell all the . . . neighborhood . . . My friend was born in a Muslim family, so it's more difficult. . . . If her family knows it, and if neighborhood knows it, she said to me that it would be the end of social life for her family." (P10)

This demonstrates how closely related privacy and physical safety are: if privacy goals are not met, it may lead directly to physical danger.

Legality. For some participants, safety stems from working legally and having access to support services:

> "I want to be recognized as a legit business. I want to tax my income and also deduct my expenses. I

> want to qualify for social security. I also want a safe way to advertise and find clients. I want to be protected by law, if a client misbehaves." (P6)

S22 describes how working in environments where clients feared law enforcement — because the location where they were pursuing services was not in compliance with legal regulation — makes their job less safe:

> "[I want] to work as little as possible in 'gray / dark' environments, such that customers [don't] have the feeling of needing to hide - [then] it is easier for me to vet them ahead of time." (S22)

For some participants, like P6, safety meant being able to call the police if they had a negative experience or were in danger. However, among our participants the ability to call the police safely might depend on whether they were officially registered as a sex worker, which was often, in turn, related to their immigration and work authorization status. Thus, some participants instead described safety as minimizing contact with the police as much as possible. S2 explains:

> "One of my sex worker friends is an undocumented migrant... She has no right to access healthcare. She is very distrustful of police and the authorities. She guards her privacy and anonymity more than other sex workers I know." (S2)

Access to community. Having access to a support community of other sex workers can also be an important component of safety. These support communities may be online or offline, as suggested by other work on sex workers [22, 64]. These online spaces can provide emotional or logistical support in the case of a negative experience, or just a place to feel validated and less isolated. S52 identifies that to feel safe, it is important for them to *"ensure I get things off my chest... with other sex workers in-house or online when I can."*

While these communities can provide safety education and resources, participants may face significant barriers to achieving and maintaining them. Policies regulating the use of online platforms for sex-work-related topics, even if not used for sex work itself, threaten the existence of these communities.

4.2 Perceptions of Risk

We next discuss the sources of risk identified by our participants. Unsurprisingly, clients pose a significant threat. Risks from clients often manifest on multiple safety axes. For example, clients may violate a sex worker's boundaries by finding their personal Facebook. If the sex worker's legal name is exposed, this can create risks of stalking and blackmail, which in turn increases risks to their physical security.

However, risk also stems from the legal and technical landscape in which sex work is conducted. Laws that regulate sex work (or business more generally) create opportunities for unwanted information exposure. Similarly, digital platforms create information exposure risks through the ways they moderate content and (dis)allow sexually-explicit uses, which may threaten the financial security and physical safety of participants. Finally, even the non-sexual policies of digital platforms — like "real name" requirements and people recommendation algorithms — create privacy risks for sex workers.

Risks from clients. Clients were often the most direct threat to workers' *physical safety*. Several participants shared stories of physical assault, while many others discussed experiences with harassment and stalking:

> "If you decide to close the [work] relation[ship] [some clients] become obsessive. A couple of times... I have been blackmailed, threaten they'd expose my activities online to my peers and family. Others have just showed up on my place of work looking for me... It's very unsettling, but with the right precautions I've learnt to avoid it. I'd much rather lose money than meet someone with potential to cause problems." (P17)

Efforts to avoid dangerous clients may threaten a participant's *financial security*. Furthermore, the threat of stalking and blackmail from clients often led participants to not only focus on physical safety, but also discuss the importance of *privacy*. In particular, keeping their real name and location private from clients was important for staying safe both online and offline. As P11 stated, *"I don't want clients to show up at my university or worse, at my flat. Some clients can get attached."* P24 had similar concerns, and shared a story illustrating the intersection between *privacy* and *physical safety*:

> "My lovely partner, who is also a photographer, has photographed me a couple times. I wasn't very smart and published my photos with his tag on a relatively public forum... Then, a client of mine who was very fond of me — which I also wasn't totally aware of — did some research and figured out who my boyfriend is. He found our places of business and then of course knew what we do in our free time, what our names are... Since then, I pay extremely close attention which tag is on the pictures." (P24)

While some negative experiences with clients may pose physical safety risks, other participants described clients threatening their *boundaries* by draining workers' time and resources: "time-wasters" just looking to chat or ask for photos without intending to book a session.

Legal risks. The extent to which sex work is legalized, and how it is regulated, influences how safe many sex workers feel

while working. Our interview participants worked primarily in Germany and Switzerland, where sex work is legal, but several had also worked abroad in countries with different legal frameworks. Their experiences both in Germany and Switzerland, as well as abroad, highlight that the different ways *legality* is defined impacts their safety. Several participants noted that when countries follow the Nordic model, in which selling sex is not illegal but buying sexual services is [59], they feel less safe. Our survey supported this: two-thirds of respondents reported that whether they were legally permitted to work as a sex worker affected how safe they felt. One participant explained that this was because clients are more afraid and less willing to share their real information with sex workers when the client is buying illegal services; sex workers rely on this information to vet new clients, or to check that an unknown client does not have a bad reputation among other sex workers [7, 67]. P10 described related challenges from working in France:

> "If guys want to see escorts they [must] pay like 1,000 Euros if they are [caught]. So that makes the job more difficult because you have to stay in this in secret. . . . If you have a problem you can't [call] the police." (P10)

Even when working in a country where sex work is legal, a worker's immigration status may prevent them from legally registering as a sex worker. Of those we surveyed, 20% reported that they felt "insecure" or "very insecure" because of their immigration status. In particular, our participants described how the inability to work legally due to immigration status or the country's legal framework results in a lack of access to law enforcement, trustworthy clients, healthcare, and other safety nets, leading to risks to *physical safety*, *respect*, and *financial security*.

Even among those who are eligible to work legally, discomfort with the way legalized sex work is regulated can create safety issues. For example, as of 2017, German sex workers are required to register in order to work [10]. Some participants worried about how the government might use such data about them. Two participants shared that the registration requirements reminded them of the Nazi era:

> "The registration and the new law, that concerns me. . . . I don't want to give them all my data. . . I feel like I'm in the 30's. Of course I have concerns about that. . . [will] the moment ever come where there are like, online raids and people try to track our profiles?" (P12)

P26 had similar thoughts, and said, *"maybe the [registration] data isn't being mishandled today, but in the future it could be."* This highlights the tension between *legality* and *privacy*; in order to be compliant, sex workers in Germany must sacrifice personal information that they may feel puts them at risk.

According to P16, the registration requirement also creates divisions between sex workers and makes it more difficult for sex workers to organize together, as their goals and needs are different. This creates barriers to building *community*, which in turn creates a barrier to staying safe:

> "There is absolutely no worker solidarity between the German workers and the non-German workers. They're happy for all of us [non-German workers] to basically die in the gutter, and it's very frustrating. I blame the way that the laws are set up in Germany, because it puts sex workers into two camps, those who are legal and compliant with German law, and those who. . . still need to work, but they can't get licenses." (P16)

Several of our participants also expressed anger at the ways FOSTA-SESTA impacted their work even in Europe. FOSTA-SESTA is a 2018 law passed by the United States Congress, which was purportedly designed to remove protection from liability for websites that facilitate sex trafficking. The effect was that many sites that sex workers had used to advertise, screen, and build community, including Backpage.com, were taken down or categorically excluded sex work from their platform [3, 12]:

> "Backpage was really great and SESTA/FOSTA really sucks. . . especially here in Germany where my job is totally legal and I pay taxes. Pretty frustrated. [It used to be] about 30% of income and I still didn't recover from it. Backpage was very easy to use for clients." (P13)

P2 worried that FOSTA-SESTA and similar laws would soon block them from all platforms they use to do sex work:

> "When I see stuff like FOSTA, it's also a question of time and when Europe will become similar. And then there'll probably be nothing left for us except to manage everything by hand." (P2)

Non-sex-work-specific laws also impact the safety of sex workers. For example, Germany has an imprint requirement for websites ("Impressumspflicht"), requiring websites to list the website operator's legal name, address, and contact information [17]. Many participants mentioned that this requirement threatens their *privacy* and potentially their *physical safety* because they must either list their real contact information on a site on which they otherwise use a pseudonym, or risk being in violation of the law.

Risks from digital sex-work platforms. Even digital sex-work platforms pose safety risks to sex workers. Several participants reported having their intellectual property — photos of them or composed advertisements they had created — stolen and republished on other sex-work advertising websites

that they had never used before. The business strategy of these websites is to steal workers' ads with legitimate photos and contact information in order to draw in customers, hoping that when the sex worker whose content has been stolen begins receiving calls from clients who found them on the new site, they choose to begin using the website in earnest. Sometimes, these new websites use workers' photos to advertise services the sex worker does not actually offer, creating risks to their *physical safety* if a client contacts them expecting those services. The participants to whom this happened described having their content stolen as an upsetting violation of their *boundaries* and *privacy*. Potential recourse, which might involve commissioning a lawyer to send a take-down notice, was described as "too laborious" (P14) or unlikely to be successful:

> "I haven't been able to get mine down. . . . I know a lot of people have [tried very hard], and they don't take them down. And that's the thing with being criminalized, it's like where do we even turn? No one cares about people stealing your stuff." (P18)

Risks from other digital platforms. Sex workers also experience harm on non-sex-work digital platforms due to platform rules and community standards. American-based digital payment platforms, like Paypal, are especially challenging for sex workers. Paypal offers a popular and simple way to transfer money, but is not a reliable tool for sex workers. Many of our participants reported having accounts frozen or deleted, sometimes blocking access to their funds. This is likely done under Paypal's "Acceptable Use Policy," which prohibits "transactions involving. . . certain sexually oriented materials or services" [58].

The lack of reliable, common payment platforms, and the risk that popular payment platforms like Paypal will freeze or disable their accounts, sometimes left our participants with difficult choices for processing payments and made *financial security* more difficult. While many still use cash primarily, cash posed challenges for large payments and for digital sex work. We discuss participants' strategies for working around these limitations in Section 4.3.

Even when workers do not use digital platforms for sex work, they may experience harms due to their identity as a sex worker. Many participants talked about how they could not use American social media platforms to discuss, let alone advertise, their legal sex work services because these platforms had rules against sexually-explicit content. One participant shared their experience of being banned from a social media platform without warning or notice:

> "I had I don't know how many followers on Instagram and at some point. . . it was just deleted. . . that definitely hurt my business . . . since a lot of clients say, yeah, where can I find pictures of you or something and then I would just send a link to my Instagram account and that was convenient." (P4)

As P20 put it, *"Google is now a market driver and one has to submit to their 'norms.'. . . Or Facebook."* In many cases, there is no recourse to being banned [5, 7].

Similarly, two participants talked about being banned from AirBnB, despite never using the platform for sex work — as far as they can tell, their identity as a sex worker alone was enough to get them permanently banned from the platform:[5]

> "AirBnB bans workers just for being [sex workers]. They have not shown their face, don't use same email or phone. . . and they don't [do sex] work from [an] AirBnB and they got banned." (P13)

While digital platforms such as PayPal, Facebook, and AirBnB are based in the U.S., they operate at a global scale. The imposition of American-driven community standards on sex workers working legally has significant repercussions for nearly every aspects of workers' safety we identified above: physical, financial, privacy, and the ability to set boundaries and create and maintain community.

Digitally-mediated interpersonal risks. Digital platforms can also enable or facilitate risks to sex workers from other platform users. Several participants described challenges with platforms that require them to share their legal name. P3 explained how this made Paypal dangerous by exposing their legal name to clients when they pay:

> "Being able to use Paypal would be awesome. . . [it doesn't work because] we're all criminals. And I work under an alias. Paypal doesn't allow that. Paypal and also Amazon are U.S.-led companies. You'll be kicked out if you do sex work" (P3)

These "real name" policies have long been documented as dangerous or damaging, for example for trans people who have not had a legal name change [16,29]. For our participants, many of whom use an alias when they work for safety purposes, such policies risk exposing their legal name to clients, and thus threaten participants' *boundaries*, their *privacy*, and potentially their *physical safety* by increasing the risk of stalking or blackmail.

Instances of digitally-mediated context collapse, in which a platform forces the intersection of previously distinct audiences [44], had similar consequences on our participants' goals. Multiple participants discussed having clients contact them through a social media or dating site that they did not use for sex work, or friends and family finding their sex work accounts. Sometimes this is a direct result of platform design

[5] AirBnB filed patents for technology that allows them to identify sex workers and those that are mentally ill in 2018 [18], but reports surfaced regarding AirBnB discriminating against sex workers as early as 2016 [57].

rather than deliberate snooping. For example, Facebook's People You May Know (PYMK) algorithm is known [32, 71] to cause this issue:

> "I wanted a second account with Facebook [for clients to interact with me]. I had a different email address... I didn't want my friends to see it at all, but they were suggested to me [by Facebook] immediately... [so] I just deleted it right away." (P29)

Regardless of the mechanism through which a sex worker is found, the experience is violating and threatens workers' established *boundaries*:

> "Somebody found my [private] Tinder profile. ... I did simply explain to him that I found that a bit stalking-like what he was doing. And that I didn't appreciate such personal contact. He carried it so far to search and find my private Facebook profile, then I blocked him. I don't want to have personal contact with my clients on my Facebook profile.... That also destroys my image as dominatrix." (P21)

While some described strategies for avoiding these privacy violating experiences (see Section 4.3), others shared this sentiment with P23: *"there are things that are just unavoidable."*

4.3 Safety Strategies

Many participants took steps to meet their safety goals and avoid potential threats to those goals. Rather than being technically complex, participants mainly relied on manual protective strategies, such as vetting clients, self-censorship, and keeping two separate devices. While technology made some of these strategies more effective, few participants relied on security tools to be safe online. Often this was due to security tools and features being a burden, disrupting other safety strategies, or being difficult for clients to use, leading to a lack of adoption or abandonment.

Covering. A common strategy our participants used to protect their *physical safety* is to "cover," or tell a friend or colleague the details of an appointment beforehand, so that they can contact the police or another emergency contact if the person does not check in at a pre-planned time. This strategy was used by 68% of our survey respondents. P2 described their strategy, and how the Internet helps them feel safer:

> "Someone almost always knows where I am. I'll put out some updates in regular intervals, call someone or do a video chat or something. ... My safety system without the Internet would... not completely fall apart, but... it wouldn't be as comfortable. And also not as comprehensive." (P2)

However, the effectiveness of covering depends on having a reliable contact to provide cover, and on being diligent about checking in while at the appointment. P5 shared a story about forgetting to check in with their contact:

> "In the heat of the moment I forgot to check the time and then someone knocked on the door and there were two men and the hotel manager at the door and it was then, of course, super embarrassing." (P5)

Several participants described wishing that there were better mechanisms for doing this without needing to depend on other people, which can be cumbersome and unreliable. P27 envisioned an app or other digitally-mediated platform that could possibly fill this role:

> "Especially for women... [who] don't speak the language. ... they would enter where they are and for how long and they could push a button to say that they're there. And then after the time runs out again, that they're out again. Of course, with a generated password each time. When that doesn't happen... the person that you entered as an emergency contact gets contacted by the app. If you don't have anyone, then it's the administrator that alerts the necessary authorities." (P27)

P27 also suggested that if this type of covering tool existed, it would also work as a deterrent for aggressive clients, and that *"probably it would be enough, if johns knew that there was something like that."*

Vetting clients. Some interview participants talked about vetting clients prior to meeting them in person, and 51% of survey respondents said they gather information about clients before meeting them.

Vetting can take two forms. In the first form, sex workers use their networks to check information from the client (for example, name or phone number) with friends or in private online forums, in order to see whether a client has a bad reputation among other sex workers or had been reported for being violent. These forums might contain others' reports of negative experiences, complete or partly obscured phone numbers, or physical descriptions of bad clients, similar to the *Bad Client and Aggressor List* described by Strohmayer et al. [67].

One participant mentioned the National Ugly Mugs, which maintains a large, centralized digital services for reporting and searching clients in the U.K. [55], but expressed frustration that the service only covered the U.K. In Germany and Switzerland, our participants did not mention such a centralized service, and several complained that the lack of such a service made vetting clients difficult.

Participants reported that vetting networks and platforms — centralized or otherwise — were not without issues, such as incompleteness or inconsistent formatting of data that makes search difficult.

Vetting also depends on the ability of the worker to get accurate information about the client before meeting them. Some participants reported that clients' willingness to share information depended on buying sex being legal, as fear of being caught would lead them to hide their information. P2 described facing several such challenges when vetting clients through shared online databases:

> "It's always dependent on what information I'm provided with... If I don't get anything, then I can't search for anything. ... The problem with that is that there's really no databank. There isn't anything standardized. [It] would just be better, if it would run centrally. And that there would be standards. A main problem with those forums is that the phone numbers are never consistently entered." (P2)

In the second form of vetting, the screening process is less about checking for previous bad behavior, and instead intended to *"separate the wheat from the chaff"* (P20). This type of vetting was also reported by Moorman et al. [54]. This was often a strategy developed over time and through trial-and-error, and might be beneficial in both protecting their time and finding respectful clients. P6 described how this process also helps filter out clients who might push other boundaries as well:

> "I optimized my contact method over the years to find a system that provides me with a way to weed out idiots. Making it quite high maintenance to contact me — [by making them contact me] in a very particular way — makes it easier to make sure that those who follow my protocol really want to book me. ... In my experience, if I have high obstacles and people are willing to take them, I can expect them to also follow my [other] rules later." (P6)

With both forms of vetting, participants said they used blocking features liberally when clients or potential clients were rude or pushy with their boundaries, e.g., within WhatsApp, on advertising platforms, or for phone calls and SMS.

Managing digital identities. *Privacy* is a critical safety goal for many sex workers, and also a goal that helps to facilitate other safety goals including maintaining *boundaries* and protecting *physical safety*, for example from stalking. Sex workers' efforts around digital privacy and security largely focused on ensuring that the digital identities used for work could not be connected back to their legal identity or contact information and ensuring separation between different digital identities.

To protect their identities, many participants described using an alias while doing sex work, and 77% of our survey respondents reported using a fake name or otherwise concealing information about themselves from clients. One worker even developed a service that would allow them, and other workers, to avoid using their real name and address while satisfying German website imprint requirements: *"I helped to develop and offer a service where sex workers can use the official union address as their address for their websites to secure their privacy"* (P6). This is one example of how having access to a community, in this case a workers' union, helps promote safety.

Some sex workers are "out," or public about being a sex worker in their personal lives. However, being out is not a binary; multiple participants who considered themselves "out" still had family members who did not know, or social contexts in which they did not want to be known as a sex worker. For example, P3 said they don't worry about sex work advertising sites collecting personal information, but at the same time they are careful about keeping some personal information off of other platforms:

> "I try to keep my real name out from Facebook. My dad is on FB and he doesn't know what I do. My address, where my boyfriend lives. He works for the church. That is not allowed to come out... My [website] imprint is through a third party." (P3)

P14 also explained how being out does not necessarily mean that clients know their personal information: *"It's actually strange, because I'm 'out' privately, but none of my clients know my real name or my address."*

As an alternative to providing false information, or not providing information at all, some workers provide details that have an element of truth but still protect their privacy. For example, P19 described how sharing information that's close to accurate but still vague helps their business by making clients feel special or trusted:

> "It's also a marketing strategy. A lot of guests are also interested in the person behind the dominatrix, so I give them something to 'chew on.' " (P19)

Finally, many participants protect their privacy by maintaining multiple digital profiles (one or more for work and one for personal use) and attempting to keep those profiles separate through the use of separate accounts or even devices (66% of survey respondents):

> "I had only one mobile for a long time, but then [I got another one]. ... You give your number to people, and at one point they come up with the clever idea to google the number, so they can see immediately what you do for a living. ... And I started to work a lot with WhatsApp statuses. And then there is the problem that if you want to post a WhatsApp status for work, you want maybe a picture that is a little bit more suggestive. And it is not so good if your private circle of friends sees that, because not everybody knows what you are doing." (P21)

While keeping separate devices was common, it is also burdensome, and not all participants chose to do it over the long term:

> "For a long time I had another phone with a different number and different WhatsApp but then I noticed that it was just too much work for me, separating them. And then I was also really slow to get back to [clients]. Then that went under and I just found it easier to just have one number." (P12)

P18 describes the cost of keeping separate identities:

> "I mean obviously I wish that sex work wasn't considered shameful and I could post to my heart's delight. It's also time consuming and it's annoying, stressful. It's like even though my family knows, I know it would be embarrassing to them if I came out as a sex worker, for them to have to explain that to their friends. That's bullshit, but it's true. It's stressful having all these phones and personas and things I have to remember. I'm like, 'Shit, did I miss that when I put this up?' All the time." (P18)

Beyond finding it difficult or not worth their time, participants also mentioned that financial incentives might motivate them to make exceptions to otherwise keeping their digital accounts or devices separate. For example, P1 described a client who found their personal social media account, an action for which they would normally block a client. However, for one particular client, they said: *"He added me [on social media] after he spent [a lot of money] in a 3 days row :D can't really be mad at him :DDD"*

Self-censorship. While our participants sometimes had considered reasons for relaxing or changing their rules around keeping separate identities, the consequences of digital identities merging or linking back to participants' personal lives or information can be significant. In order to avoid this, some of our participants went beyond maintaining separate profiles, or using false names, to minimizing the amount of information they have online at all.

Out of fear that clients will find their personal Facebook profile or be recommended to them through PYMK, P13 decided to keep their information on the profile extremely limited: *"I don't have photos. I don't have my city or school or uni."*

Keeping photos off of work accounts is more difficult, as the photos are used to advertise. For these accounts, our participants protected their identities by carefully curating photos so that their face or identifying features like tattoos were not visible (46% of survey respondents).

Participants also mentioned removing content from their phones before crossing borders, for fear of being searched and deported. P18 went as far as to completely shut down their online accounts when traveling:

> "I delete my whole work phone, everything incriminating on my computer. I take down my website, I take down all my apps. . . . If they feel suspicious for some reason as I'm crossing and they search all my stuff I don't want that to lead to getting deported." (P18)

This practice was mentioned even by those working legally:

> "I am legally allowed to work in most countries where I work. [However,] I am scared of getting banned from certain countries just for being a sex worker so I remove all my info, account and website and wipe my phone before travelling." (S11)

However, as with keeping separate devices, some participants stopped using such measures because they were too cumbersome or felt ineffective. P16 describes the decision to no longer hide their face in photos:

> "I used to always blur out my face, which I don't do anymore. That was a conscious decision that I knew would make me less safe. . . . I was tired of doing a lot of photoshopping, and partly because I felt a little bit safer in my work at the time, which I don't know if I do anymore, but. . . you can't take back. And clients connect very strongly with faces, so it's a good marketing move." (P16)

Managing security & privacy settings. Few interview participants depended on privacy and security settings within their devices or online accounts to stay safe online. This was reflected in the survey, where only 35% of respondents reported changing security and privacy settings to be more private or secure.

Of interview participants who did discuss modifying settings, the two most commonly mentioned settings were visibility settings on Facebook and location settings on mobile devices. These settings, reasonably, correspond to some of the more tangible physical risks that participants face — being outed unintentionally, and being located or stalked. P18 explained how they changed their privacy settings to avoid being found on Facebook:

> "I used to get a lot of 'Do you know this person' about clients, even though we never interacted on Facebook. I've never interacted with these clients on Facebook and I don't remember their real name or anything, but they would pop up. . . . It's not so good. I had to make everything private." (P18)

A few participants expressed doubt that security and privacy settings would be effective. As P8 put it, *"If we are online, there isn't a lot of hope for privacy."* P21 explained that they do not trust privacy settings, and instead will opt for physical or hardware solutions such as removing a phone from a room,

or using multiple devices, to make sure their mobile phone does not collect information they do not want it to:

> "I don't really trust the whole system in this respect. I think it doesn't matter if you put [settings] on or off. In case of doubt the phone will listen in, go along, take notes. Sometimes, when I have to talk about something, I mind that there isn't a phone in the room." (P21)

That people do not or cannot rely on in-platform settings to regulate their boundaries has also been observed in the general population [73].

Security-focused tools. Similarly, few participants mentioned using tools specifically built for security and privacy. In our survey, we asked whether they used several security tools: encrypted messaging applications like WhatsApp or Signal (32% reported using), a VPN (14%), encrypted email (9%), Tor (9%), Password Managers (8%), or cryptocurrency (5%). Interview participants reported two main barriers to using such tools: feeling that the tools were too challenging to use — either for themselves or their clients — or feeling that the tools were not sufficiently effective given the effort necessary to use them. P21 describes a friend setting up encrypted email for them, which P21 no longer uses:

> "I have an acquaintance who [will] only write encrypted emails, but that's very effortful. . . . [They] had to download an extra program for me. There you always had a key and then you had to mess with it forever until you could read that email, this was way too stupid for me." (P21)

Security tools can also get in the way of participants' work or other safety goals. P16 explained that they previously used a VPN to obscure their location, but stopped because it created new privacy risks and interfered with their business:

> "Many VPNs will sell your data. Also, many of the advertising platforms either are partly location-based or won't let you use their services if you're not coming from the country that they're based in. One of the U.K. [sex work advertising] platforms. . . you have to have a local phone number and be accessing that website from an IP within that country." (P16)

Particularly of note, although many of our interview participants described having problems with payment processors and two even lamented the lack of anonymous payment platforms, none described using Bitcoin or another cryptocurrency. P3 said, *"I'm not enough of a techie for that. . . [and] nobody's ever suggested it."* Instead, most sex workers relied on cash. How well this works, of course, depends on their type of sex work (e.g., cam performers cannot collect cash from viewers).

Further, even if a sex worker felt they were sufficiently skilled to use a security tool, and felt that the tool was sufficiently beneficial, their clients may lack the digital skill or interest to use such tools. One survey respondent commented on our list of protective strategies:

> "I would gladly do all of the above, but that really only works when the customers participate: Threema / Signal / Telegram, PGP-encryption, cryptocurrency..." (S49)

As S49 points out, all parties must use it before a new tool like a messaging app or payment system can be useful. This barrier of needing others to also comply with a security protocol was similarly identified by journalists looking to communicate securely with sources [50].

Resignation and regret. Finally, some of our participants expressed resignation or apathy about safety. Some participants felt there was little they could do to be *"100% safe at this job"* (S15). This led some participants to disregard safety practices because they felt that the behaviors are not effective or that harm is inevitable — a common response to corporate surveillance [20]. P25 said:

> "When I think about it, it's like how safe are you, really? How protected are you, really, when Google can find you anywhere, Facebook can find you anywhere? I think the aspect or the perception of safety is a little like, you can be found if someone really wants to find you. It's not so difficult anymore, especially with online presence and everything else. It really depends what you're trying to achieve." (P25)

P13 described how despite the serious risks for them, keeping accounts separate in the course of using them day-to-day felt impossible:

> "I login to Kaufmich [a sex-work advertising site] in browser on my personal phone and my Apple account for work phone is registered to my passport name. . . . I hate myself for it sometimes. . . . This stuff could get me killed or deported. . . . I am not prepared." (P13)

Several other participants similarly described feeling regret about taking insufficient precautions. Some expressed that they had originally made choices they felt were unsafe when creating an account, but now felt stuck with those choices; as P16 put it, *"You can't erase what you've done on the Internet."* This sense that it's impossible to correct past mistakes may keep some workers from engaging in more careful privacy management in the future.

5 Discussion

Sex workers experience salient risks both offline and online. Our findings show that our participants have nuanced and multidimensional conceptions of safety and a clear understanding of both digital and offline risks. While physical security was a critical part of safety, safety also included financial security, respect, privacy, legality, clear online and offline boundaries, and access to a community that could help support safety practices. Participants' safety strategies must thus simultaneously support multiple safety goals.

We further identify the primary sources of risk and safety strategies of this high-risk population, who often need to use the Internet to do their work but also face significant consequences if their strategies fail. While our participants have well-developed sex-work-specific protective strategies like covering and vetting clients, many online strategies relied on logical or physical mechanisms — e.g., having two mobile phones, carefully keeping photos with their faces off the Internet, and self-censoring in both work and personal online spaces — rather than using, e.g., platform integrated privacy settings. Few participants used dedicated security tools, and those who did were likely to abandon them, either because they felt the tools were more work than they were worth, or because they disrupted competing work and safety goals.

5.1 Building for sex work.

Ultimately, many of the risks our participants face are not solvable by improved privacy and security tools. Instead, explicit discrimination by social media and payment platforms, poorly designed and explicitly anti-sex-work laws, as well as stigma from the general population, contribute to a dangerous work environment for sex workers. Solutions to the largest problems depend on collective action leading to changing perceptions of sex work, policy changes, and legal changes, rather than the strategic deployment of technical solutions.

With this in mind, we identify two primary ways in which technical tools can enhance sex worker safety. First, existing tools could be modified to accommodate the use cases and threat models experienced by sex workers. Second, new safety tools that specifically address currently unmet sex worker needs can be created.

Refining existing tools. Existing tools are especially well positioned to address *surveillance* risks (e.g., at the border while traveling internationally, by police or governments, or by cross-platform tracking and data aggregation). However, upon examining why these tools are not widely used, we found that many violate other critical safety goals.

In particular, encrypted messaging tools like Signal and WhatsApp could help sex workers keep message content private from both government and corporate surveillance.[6] However, because both applications only allow a single profile per phone number, safely using Signal or WhatsApp with both work and personal contacts might further depend on having a second SIM card or phone, lest the wrong audience see the wrong name or profile photo. In this case, an application with otherwise desirable security properties (e.g., end-to-end encryption and blocking features) becomes harder to use safely for someone with a need to communicate simultaneously with disparate audiences. This design is not necessary for the functioning of the tool — either app could likely enable some limited number of profiles per account without necessarily sacrificing other security properties like end-to-end encryption.

Similarly, VPNs and Tor may offer some protection from surveillance, but their value significantly decreases when they disrupt the user's ability to access the forums or platforms they depend on to stay safe, as one of our participants experienced when they were unable to access geolocation-based vetting platforms. Platforms that manage access through IP location risk denying access to legitimate users who need a VPN [47].

Protecting workers during interactions with clients is another space in which existing digital security and privacy tools have the potential for impact. The safety goals here are usually to keep personal information from clients, keep work information from family and friends, and to be able to draw boundaries and cut off contact with clients when they become aggressive. In these cases, having access to fine-grained privacy and visibility settings may help some workers (those who know about them and trust them), but our participants found that even this careful management fails due to invisible data aggregation, resulting in being outed through people recommendation algorithms or having personal accounts blacklisted because of their work account's activity. Over time, failure seemed inevitable. These issues suggest that many social media platforms continue to fail users who have multiple identities to manage, and that reviewing and changing a platform's data-use policies can be as critical as creating intuitive front-end settings.

Finally, one major risk to workers' financial security, a dimension of safety, was lack of access to digital payment platforms. Cryptocurrencies offer anonymous digital payments and thus might seem like an obvious solution. However, virtually none of our participants used tools like Bitcoin. Cryptocurrencies introduce additional difficulties: getting clients to use such services, even if workers are comfortable using them, and the need to convert between currencies in an already-difficult banking situation. Thus, the vast majority of our participants turned to the analog solution, cash, despite having its own set of problems.

In this case, cryptocurrencies serve as a useful example of how questions of access and usability are not the first

[6] WhatsApp no longer keeps messages to businesses private, and continues to degrade user protection from corporate surveillance [19]; we include it here because at the moment it remains the most popular encrypted messaging application.

that researchers and technologists should ask when building or improving security tools for high-risk users. Rather than considering how we can make cryptocurrencies easier to use for sex workers and clients, we should consider whether they are addressing the fundamental need in the first place. For many, they do not. Our participants need simple anonymous payments, but Bitcoin and similar tools are massively complex systems that do not provide anonymous digital cash. Instead, they provide an entirely independent currency that fluctuates wildly, requires currency brokers and new accounts, and puts users at risk of a massive network of targeted attacks seeking to steal account credentials.

Opportunities for new tools. As articulated by our participants, there may also be opportunities to build bespoke safety tools that better support sex workers specifically.

For example, P27 describes their ideal covering app, which could help sex workers stay safe without a dependable community. Additionally, while there are no technical mechanisms currently available to prevent photos and ads from being copied and republished, there may be opportunity for automating copyright take-down requests for major sites that steal and republish content.

Usable safety tools for sex workers have the potential to support the safety and independence of a sizable population. However, as can be seen from other security tools, if not well-grounded in the experiences of sex workers and their particular legal context, tools can be at best useless and at worst harmful. Design and operation of new tools and platforms should include, and ideally be led by, sex workers. Several sex work and technology collectives like Assembly Four [6] and Hacking//Hustling [28] offer models for this type of collaboration.

5.2 Designing across diverse populations.

In many instances, sex workers provide another data point showing that many common digital mechanisms can amplify risk and complicate protective strategies. In other instances, however, their needs may diverge from other high-risk populations. This tension should be considered when looking to design for a given community and in building general-purpose tools.

For example, being able to use a pseudonym or keep profiles unlinked from their legal identity is critical for the safety of many of our participants, as it sometimes also is for trans people [16], drag queens [52], and intimate partner abuse survivors [45], among others. Our findings underscore why identity management online is an important security and privacy issue, and may suggest that allowing users to have fully pseudonymous profiles — that is, even unlinked from emails and phone numbers that could be used elsewhere — may reduce the risk of digital boundary violations that lead to stalking and harassment [48]. Even in cases where users do the work to keep profiles separate, unwanted and unexpected intersections of work and personal identities online through friend recommendation algorithms or through being identified by use of a shared, single phone number or email across personal and work platforms can cause significant problems.

At the same time, sex workers themselves depend on having the real — or at least persistent — contact information for clients to vet them and keep track of their behavior and preferences. If fully pseudonymous or anonymous profiles were in place on many of the platforms sex workers use, they could find themselves facing new safety challenges, as existing vetting systems may fail. Furthermore, anonymity on social networking sites can enable further abuse and harassment, which is frequently levied against women, minorities, and other marginalized groups [70].

5.3 Broadening the scope of security.

Beyond designing specific technical tools, our results underscore the multidimensional nature of digital safety. Our participants had well-defined ideas of what they needed in order to stay safe. However, many of the elements that were central to their safety goals, like financial security, boundary regulation, respect, and even physical safety, are often not central to the design and study of security and privacy tools and experiences. Our work adds support to a growing body of evidence [23, 24, 30, 33, 41, 46, 61, 70] that online safety involves axes beyond — but intertwined with — digital security and privacy. Thus, we encourage future research and development to holistically consider the multi-dimensional aspects that comprise users' safety experiences. Security researchers and developers must revisit their assumptions about risk and benefit to better align with the needs articulated by their users [40].

6 Conclusion

Through interviews and surveys with sex workers, we examine sex workers' safety goals, their perception of risks to those goals, and the behaviors they employ to mitigate these risks. Our participants expressed that their safety was defined across multiple interrelated axes, and they perceived risks to their safety from clients, platforms, and legal entities. Our results suggest that sex workers are not only aware of the risks presented by digitally-mediated sex work but are also employing multiple ways to protect privacy and security while online. However, they often rely on manual strategies, such as using multiple devices, as current tools do not balance effort and efficacy well enough to address their safety needs and goals. Our findings demonstrate the importance of studying high-risk populations, in order to develop better security tools to protect both those populations and users in general.

Acknowledgments

We thank Eszter Hargittai, Sean Kross, Maggie Oates, and Anna-Kathrin Marx for their invaluable support on this project. We would like to acknowledge support from the Max Planck Institute for Software Systems, which funded study costs and materials for this project.

Elissa Redmiles was supported by the University of Zurich, the National Science Foundation Graduate Research Fellowship Program under Grant No. DGE 1322106, and a Facebook Fellowship for her time on this project. Allison McDonald was supported by a Facebook Fellowship for her time on this project.

References

[1] Ruba Abu-Salma, Elissa M Redmiles, Blase Ur, and Miranda Wei. Exploring user mental models of end-to-end encrypted communication tools. In *8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18)*, 2018.

[2] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. Obstacles to the Adoption of Secure Communication Tools. In *2017 IEEE Symposium on Security and Privacy (SP)*, 2017.

[3] Kendra Albert, Emily Armbruster, Elizabeth Brundige, Elizabeth Denning, Kimberly Kim, Lorelei Lee, Lindsey Ruff, Korica Simon, and Yueyu Yang. Fosta in legal context. Available at SSRN: https://ssrn.com/abstract=3663898, 2020.

[4] Sean T Allen, Katherine HA Footer, Noya Galai, Ju Nyeong Park, Bradley Silberzahn, and Susan G Sherman. Implementing targeted sampling: lessons learned from recruiting female sex workers in baltimore, md. *Journal of Urban Health*, 96(3), 2019.

[5] Payal Arora. Decolonizing Privacy Studies. *Television and New Media*, 20(4), 2019.

[6] Assembly Four. Empowering sex workers through technology. https://assemblyfour.com, accessed 2021-02-16.

[7] Catherine Barwulor, Allison McDonald, Eszter Hargittai, and Elissa M Redmiles. "Disadvantaged in the American-dominated internet": Sex, Work, and Technology. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021.

[8] Adam Beautement, M Angela Sasse, and Mike Wonham. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop*, 2008.

[9] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. Passwords and the evolution of imperfect authentication. *Communications of the ACM*, 58(7), 2015.

[10] Frauen und Jugend Bundesministerium für Familie, Senioren. The new prostitute protection act, 2019. https://www.bmfsfj.de/blob/117624/ac88738f36935f510d3df8ac5ddcd6f9/prostschg-textbausteine-en-data.pdf, accessed 2020-10-03.

[11] Tammy Castle and Jenifer Lee. Ordering sex in cyberspace: A content analysis of escort websites. *International Journal of Cultural Studies*, 11(1), 2008.

[12] Lura Chamberlain. Fosta: A hostile law with a human cost. *Fordham Law Review*, 87(5), 2019.

[13] Camille Cobb and Tadayoshi Kohno. How Public Is My Private Life? In *Proceedings of the 26th International Conference on World Wide Web*, 2017.

[14] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. "It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018.

[15] Scott Cunningham and Todd D. Kendall. Prostitution 2.0: The changing face of sex work. *Journal of Urban Economics*, 69(3), 2011.

[16] Avery P Dame-Griff. Trans cultures online. *The International Encyclopedia of Gender, Media, and Communication*, 2020.

[17] Bundesrepublik Deutschland. Telemediengesetz (tmg). https://www.gesetze-im-internet.de/tmg/__5.html, accessed 2020-10-12.

[18] E.J. Dickson. Airbnb: Who's allowed to use the popular home-sharing site? Rolling Stone, January 2020. https://www.rollingstone.com/culture/culture-news/airbnb-sex-worker-discrimination-935048/, accessed 2020-10-07.

[19] Pranav Dixit. People Are Really Mad About Facebook's Changes To WhatsApp's Privacy Policies. Buzzfeed News, January 2021. https://www.buzzfeednews.com/article/pranavdixit/whatsapp-privacy-policy-changes, accessed 2021-02-21.

[20] Nora A Draper and Joseph Turow. The corporate cultivation of digital resignation. *New Media & Society*, 21(8), 2019.

[21] J. Dutson, D. Allen, D. Eggett, and K. Seamons. Don't punish all of us: Measuring user attitudes about two-factor authentication. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, 2019.

[22] Valerie Feldman. Sex Work Politics and the Internet. In Carisa R. Showden and Samantha Majic, editors, *Negotiating Sex Work*, chapter 11. University of Minnesota Press, 2014.

[23] Antigoni-Maria Founta, Constantinos Djouvas, Despoina Chatzakou, Ilias Leontiadis, Jeremy Blackburn, Gianluca Stringhini, Athena Vakali, Michael Sirivianos, and Nicolas Kourtellis. Large scale crowdsourcing and characterization of twitter abusive behavior. *arXiv preprint arXiv:1802.00393*, 2018.

[24] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "a stalker's paradise": How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018.

[25] Kevin Gallagher, Sameer Patil, and Nasir Memon. New me: Understanding expert and non-expert perceptions and usage of the tor anonymity network. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 2017.

[26] Christine Geeng, Jevan Hutson, and Franziska Roesner. Usable sexurity: Studying people's concerns and strategies when sexting. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, 2020.

[27] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. Keeping a low profile? technology, risk and privacy among undocumented immigrants. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018.

[28] Hacking//Hustling. About hacking//hustling. https://hackinghustling.org, accessed on 2021-02-19.

[29] Oliver L Haimson, Avery Dame-Griff, Elias Capello, and Zahari Richter. Tumblr was a trans technology: the meaning, importance, history, and future of trans technologies. *Feminist Media Studies*, 2019.

[30] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. Clinical computer security for victims of intimate partner violence. In *28th USENIX Security Symposium (USENIX Security 19)*, 2019.

[31] Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*, 2009.

[32] Kashmir Hill. How facebook outs sex workers. Gizmodo, October 2017. https://gizmodo.com/how-facebook-outs-sex-workers-1818861596, accessed 2020-09-01.

[33] Damilola Ibosiola, Ignacio Castro, Gianluca Stringhini, Steve Uhlig, and Gareth Tyson. Who watches the watchmen: Exploring complaints on the web. In *The World Wide Web Conference*, 2019.

[34] Iulia Ion, Rob Reeder, and Sunny Consolvo. "...no one can hack my mind": Comparing expert and non-expert security practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015.

[35] Sandy E. James, Jody L Herman, Susan Rankin, Mara Keisling, LIsa Mottet, and Ma'ayan Anafi. The Report of the 2015 U.S. Transgender Survey. Technical report, National Center for Transgender Equality, 2016.

[36] Lisa Grazina Johnston, Keith Sabin, Mai Thu Hien, and Pham Thi Huong. Assessment of respondent driven sampling for recruiting female sex workers in two vietnamese cities: reaching the unseen sex worker. *Journal of Urban Health*, 83(1), 2006.

[37] Angela Jones. Sex Work in a Digital Era. *Sociology Compass*, 9(7), 2015.

[38] Angela Jones. "I get paid to have orgasms": Adult webcam models' negotiation of pleasure and danger. *Signs*, 42(1), 2016.

[39] Angela Jones. *Camming*. NYU Press, 2020.

[40] Seny Kamara. Crypto for the people, 2020. https://www.youtube.com/watch?v=Ygq9ci0GFhA, accessed 2020-10-15.

[41] Stevens Le Blond, Alejandro Cuevas, Juan Ramón Troncoso-Pastoriza, Philipp Jovanovic, Bryan Ford, and Jean-Pierre Hubaux. On enforcing the digital immunity of a large humanitarian organization. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018.

[42] Ada Lerner, Helen Yuxun He, Anna Kawakami, Silvia Catherine Zeamer, and Roberto Hoyle. Privacy and activism in the transgender community. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020.

[43] Gus Lubin. There are 42 million prostitutes in the world, and here's where they live. Business

Insider, 2012. https://www.businessinsider.com/there-are-42-million-prostitutes-in-the-world-and-heres-where-they-live-2012-1, accessed 2020-09-16.

[44] Alice E. Marwick and Danah Boyd. I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media and Society*, 13(1), 2011.

[45] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. "she'll just grab any device that's closer": A study of everyday device & account sharing in households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 2016.

[46] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017.

[47] Allison McDonald, Matthew Bernhard, Luke Valenta, Benjamin VanderSloot, Will Scott, Nick Sullivan, J. Alex Halderman, and Roya Ensafi. 403 forbidden: A global view of cdn geoblocking. In *Proceedings of the Internet Measurement Conference 2018*, 2018.

[48] Allison McDonald, Carlo Sugatan, Tamy Guberek, and Florian Schaub. The Annoying, the Disturbing, and the Weird: Challenges with Phone Numbers as Identifiers and Phone Number Recycling. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021.

[49] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 2019.

[50] Susan E. McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. Investigating the computer security practices and needs of journalists. In *24th USENIX Security Symposium (USENIX Security 15)*, 2015.

[51] M Giovanna Merli, James Moody, Jeffrey Smith, Jing Li, Sharon Weir, and Xiangsheng Chen. Challenges to recruiting population representative samples of female sex workers in china using respondent driven sampling. *Social Science & Medicine*, 125, 2015.

[52] Lil Miss Hot Mess. Selfies and side-eye: Drag queens take on facebook. *Studies in Gender and Sexuality*, 16(2), 2015.

[53] Matthew B Miles, A Michael Huberman, and Johnny Saldaña. Qualitative data analysis: A methods sourcebook. 3rd, 2014.

[54] Jessica D. Moorman and Kristen Harrison. Gender, Race, and Risk: Intersectional Risk Management in the Sale of Sex Online. *Journal of Sex Research*, 53(7), 2016.

[55] National Ugly Mugs. National ugly mugs. https://uglymugs.org, accessed 2020-10-04.

[56] Joint United Nations Programme on HIV/AIDS (UNAIDS), Data UNAIDS, et al. Geneva, Switzerland; 2018. *North American, Western and Central Europe: AIDS epidemic update regional summary*, 2019.

[57] Kari Paul. Why it's perfectly legal for airbnb to discriminate against sex workers. Vice, July 2016. https://www.vice.com/en/article/gvzzkx/why-its-perfectly-legal-for-airbnb-to-discriminate-against-sex-workers, accessed 2020-10-07.

[58] Paypal. Paypal acceptable use policy. https://www.paypal.com/de/webapps/mpp/ua/acceptableuse-full?locale.x=en_DE, accessed 2020-10-12.

[59] Jane Pitcher and Marjan Wijers. The impact of different regulatory models on the labour conditions, safety and welfare of indoor-based sex workers. *Criminology and Criminal Justice*, 14(5), 2014.

[60] Elissa M. Redmiles. Behind the red lights: Methods for investigating the digital security and privacy experiences of sex workers. In Eszter Hargittai, editor, *Research Exposed: How Empirical Social Science Gets Done in the Digital Age*, chapter 5. Columbia University Press, 2020.

[61] Elissa M Redmiles, Jessica Bodford, and Lindsay Blackwell. "I just want to feel safe": A diary study of safety perceptions on social media. In *Proceedings of the International AAAI Conference on Web and Social Media*, volume 13, 2019.

[62] Elissa M Redmiles, Michelle L. Mazurek, and John P Dickerson. Dancing pigs or externalities? Measuring the rationality of security decisions. In *Proceedings of the 2018 ACM Conference on Economics and Computation*, 2018.

[63] Teela Sanders, Laura Connelly, and Laura Jarvis King. On our own terms: The working conditions of internet-based sex workers in the UK. *Sociological Research Online*, 21(4), 2016.

[64] Teela Sanders, Jane Scoular, Rosie Campbell, Jane Pitcher, and Stewart Cunningham. *Internet Sex Work: Beyond the Gaze*. Palgrave Macmillan, 2018.

[65] Sebastian Shehadi and Miriam Partington. Coronavirus: Offline sex workers forced to start again online. BBC, April 2020. https://www.bbc.com/news/technology-52183773.

[66] L. Simko, A. Lerner, S. Ibtasam, F. Roesner, and T. Kohno. Computer security and privacy for refugees in the united states. In *2018 IEEE Symposium on Security and Privacy (SP)*, 2018.

[67] Angelika Strohmayer, Jenn Clamen, and Mary Laing. Technologies for social justice: Lessons from sex workers on the front lines. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019.

[68] Angelika Strohmayer, Mary Laing, and Rob Comber. Technologies and social justice outcomes in sex work charities: Fighting stigma, saving lives. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017.

[69] TAMPEP. Sex Work Migration Health. A report on the intersections of legislations and policies regarding sex work, migration and health in Europe. Technical report, TAMPEP International Foundation, 2009.

[70] K. Thomas, D. Akhawe, M. Bailey, D. Boneh, E. Bursztein, S. Consolvo, N. Dell, Z. Durumeric, P. Kelley, D. Kumar, D. McCoy, S. Meiklejohn, T. Ristenpart, and G. Stringhini. Sok: Hate, harassment, and the changing landscape of online abuse. In *2021 IEEE Symposium on Security and Privacy (SP)*, 2021.

[71] Kurt Wagner and Jason Del Ray. Facebook's 'people you may know' feature can be really creepy. how does it work? Vox, October 2016. https://www.vox.com/2016/10/1/13079770/how-facebook-people-you-may-know-algorithm-works, accessed 2020-10-07.

[72] Philipp Winter, Anne Edmundson, Laura M. Roberts, Agnieszka Dutkowska-Zuk, Marshini Chetty, and Nick Feamster. How do tor users interact with onion services? *Proceedings of the 27th USENIX Security Symposium*, 2018.

[73] Pamela Wisniewski, Heather Lipford, and David Wilson. Fighting for my space: Coping mechanisms for sns boundary regulation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2012.