Digital Technologies and Human Trafficking: Combating Coercive Control and Navigating Digital Autonomy

Sophie Stephenson
School of Computer, Data & Information Sciences
University of Wisconsin
Madison, USA
sophie.stephenson@cs.wisc.edu

Lana Ramjit
Computer Science
Cornell Tech
New York, New York, USA
lana.ramjit@cornell.edu

Thomas Ristenpart
Cornell Tech
New York, New York, USA
ristenpart@cornell.edu

Nicola Dell
Jacobs Institute
Cornell Tech
New York, New York, USA
nixdell@cornell.edu

Abstract

This paper describes a qualitative study that interrogates the types of technology-facilitated coercive control faced by survivors of human trafficking and uncovers potential interventions to aid survivors' recovery. Via semi-structured interviews with 21 participants, including trafficking survivors and professional advocates, we show how traffickers use technology as a lever for control, engaging in surveillance, blackmail, impersonation, and harassment as they compel survivors to stay in the trafficking situation. In recovery, digital footprints keep survivors tethered to their trafficking experience, impacting their digital autonomy, economic mobility, and feelings of safety. Nevertheless, technology can also be a valuable tool for survivors' recovery, connecting them to essential resources and support systems. We discuss the need for interventions and services that account for the specificity of the trafficking context to help survivors attain digital safety and autonomy, including the potential to adapt existing tech safety services designed for other contexts to human trafficking.

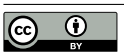
CCS Concepts

• **Human-centered computing** → *Empirical studies in HCI*; • **Security and privacy** → *Human and societal aspects of security and privacy*.

Keywords

human trafficking, sex trafficking, labor trafficking, technology-facilitated abuse, tech abuse, technology-facilitated coercive control, clinical computer security, technology abuse clinic, digital safety, at-risk users.

ACM Reference Format:
Sophie Stephenson, Lana Ramjit, Thomas Ristenpart, and Nicola Dell. 2025. Digital Technologies and Human Trafficking: Combating Coercive Control and Navigating Digital Autonomy. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 21 pages. https://doi.org/10.1145/3706598.3713544



ACM ISBN 979-8-4007-1394-1/25/04
https://doi.org/10.1145/3706598.3713544

1 Introduction

As technology advances, so does technology-facilitated abuse. Modern technologies like social media [134], Bluetooth location trackers [26, 29], smartphone apps [32, 111], multiplayer online games [46], and smart home devices [124, 125, 129] are all leveraged to surveil and harass survivors of digital violence. This technology-facilitated abuse is widespread [133] and results in harms like privacy violations [47], impacts to survivors' mental health [143], reputational damage [133], and escalating physical or sexual violence [53].

HCI and security & privacy scholars have investigated the digital safety challenges facing a variety of at-risk groups [12, 144] for whom tech abuse can be both more likely and more damaging. Studies have documented harms to survivors of intimate partner violence (IPV) [47, 48, 82], sex workers [10, 16, 83, 112, 122, 127], youth [46], activists [54], queer people [50], and refugees [117], among others. At the same time, technologists have proposed abuse mitigation strategies including changes to technology design [4, 84] and policy [64, 107] as well as initiatives to directly support survivors. Perhaps most notable are *technology abuse clinics* [39, 57, 139, 140] that connect IPV survivors with trained technologists for personalized, one-on-one support.

In contrast to other at-risk groups, researchers have *not* yet paid sufficient attention to survivors' experiences of technology-facilitated abuse in human trafficking. Human trafficking is a form of exploitation in which one person (a *trafficker*) uses force, fraud, or coercion to compel another person (a *survivor*) to perform labor, including sex work, against their will [101]. Like many forms of abuse, traffickers often leverage non-violent coercion to facilitate control and exploitation [33, 42, 63]. Traditionally marginalized groups like Indigenous people [7], undocumented immigrants [108], and people in poverty [108] are at higher risk of experiencing trafficking.

Prior work has focused on how traffickers use technology to recruit and to facilitate forced labor and, separately, on technological methods to combat trafficking. Research has shown that traffickers commonly recruit potential victims through social media/dating platforms [3, 7, 35, 46, 75] or through fraudulent job postings [3, 35];

then, they use technology to communicate with people who purchase forced labor [7, 135], post advertisements [3, 135], and exchange money [35, 95, 96]. Aware of these behaviors, researchers have attempted to design algorithms that identify survivors of human trafficking [75, 96, 102, 132] by analyzing online artifacts such as advertisements for sex work [102]—methods that are ethically questionable [22, 96] and known to harm non-trafficked sex workers [2, 44, 62].

Those lines of work do not center trafficking survivors' digital safety concerns. To our knowledge, only two papers do. Chen et al. [33] examined security and privacy in service providers' interactions with survivors, finding that providers try to make technology-related choices that protect survivors from revictimization and other harms. However, their work did not aim to understand survivors' experiences with technology-facilitated coercive control. Thorn [136] surveyed 260 survivors of domestic minor sex trafficking, gathering descriptive statistics about survivors' access to technology and how often their technology usage was monitored. Their research raises new questions for investigation, e.g., about the methods traffickers use to enact this monitoring.

Our study expands this literature by contributing an in-depth investigation into how trafficking survivors experience technology-facilitated coercive control and the impact of technology on survivors' attempts to attain digital safety and autonomy. With this knowledge, we then begin to explore whether support services from other abuse contexts—for example, technology abuse clinics designed for survivors of IPV—might also benefit trafficking survivors. Specifically, we conducted a qualitative study consisting of 21 interviews with trafficking survivors and professional advocates that investigates:

- RQ1: What types of technology-facilitated abuse do trafficking survivors face? How do they resist it?
- RQ2: How does technology impact trafficking survivors' attempts to attain lasting safety and security?
- RQ3: Which interventions might help trafficking survivors?

Towards answering RQ1 (Section 4), we detail the ways that traffickers use technology to surveil, threaten, impersonate, and harass survivors, gaining access to devices and accounts through coercion and physical proximity. For example, while prior work showed that survivors report being surveilled [33, 136], we specifically identify that traffickers use location trackers, dual-use apps, workplace surveillance devices, and even simple phone calls to overtly and covertly monitor survivors. At the same time, technology is a valuable tool for survivors to access services and get support—but doing so under technology-enabled coercion can be risky. Survivors evade surveillance by avoiding compromised communication methods and ditching unsecured devices, hampering their ability to use technology to seek help. We show that the root of this problem is the challenge of pinpointing how, exactly, a trafficker is surveilling, which we identify as a key area for intervention.

For RQ2 (Section 5), we show that although becoming unreachable to the trafficker is a top concern for survivors, they face challenges severing digital connections, hindering their real and perceived safety. Other digital footprints also persist; in addition to social media triggers identified by Chen et al. [33], we detail how lingering explicit or incriminating content greatly harms survivors' wellbeing. To attain digital autonomy, survivors often fight to remove harmful content, while others take steps to reclaim their online identity. In addition, we are the first to identify how lingering concerns around reachability can hamper survivors' economic mobility, especially since technology is often required to apply for and perform jobs.

Finally, for RQ3 (Section 6), we show a clear need for services that help survivors combat technology-facilitated coercive control by identifying and removing sources of surveillance, allowing survivors to access services. Going further, we identify specific guidelines for designing these services: for instance, a need to account for the unique severity of trafficking. In parallel, we argue that survivors need services that help them build digital autonomy in recovery, including trauma-informed technology literacy courses and tools to remove image-based sexual abuse material.

We close by situating our findings within the broader literature on technology-facilitated abuse. We discuss how many of the coercive control tactics we see in human trafficking share similarities with technology-facilitated abuse in other contexts, especially IPV. This suggests that existing interventions, including technology abuse clinics, may be an appropriate avenue for helping trafficking survivors. At the same time, we identify unique aspects of technology-facilitated abuse in trafficking contexts, such as traffickers' strategies to implicate survivors in criminal activities instead of themselves. Interventions must account for these nuances. Finally, we call on technologists to join efforts to advocate for improved laws, policies, and platform changes, including the ability to remove harmful online content, that would benefit survivors of many kinds of online abuse.

2 Background and Related Work

Here, we first provide background on human trafficking (§ 2.1), positioning sex trafficking in the context of sex work (§ 2.2). We then review related work on technology's role in human trafficking (§ 2.3) and technology safety for survivors of digital violence (§ 2.4).

2.1 Human Trafficking

Human trafficking is broadly defined as "the use of force, fraud, or coercion to compel a person into commercial sex acts or labor against their will" [101]. This encompasses many types of exploitative labor across dozens of industries, including personal or commercial sexual services, domestic work, health and beauty services, massage parlors, and even carnivals [99]. Because of its wide scope, trafficking is frequently classified into two subcategories: sex trafficking and labor trafficking. However, experts and sex workers point out that since commercial sex work is a form of labor, these categories are not mutually exclusive and often difficult to distinguish [98, 101].

Moreover, experts emphasize that while trafficking may involve physical force, many traffickers exclusively use non-violent coercion to recruit and retain survivors [33, 42, 63]. Traffickers frequently employ psychological and economic manipulation tactics, promising something a survivor needs—e.g., a job, food, a place to stay, stability, drugs, or love & acceptance—that is difficult to pass up and, if legitimate, difficult to part with. Traffickers may also displace survivors from their support system or culture, or retain

survivors' ID cards, immigration documents, or other possessions, convincing survivors that they can only rely on traffickers to survive [71]. In many instances, the trafficker might be a parent or guardian [106] or the survivors may view the trafficker as a romantic or intimate partner [14]. Whether a romantic relationship or not, close physical and social proximity grants traffickers access to personally identifiable information and socially engineered attacks like impersonation and identity theft [33]. These relational dynamics and coercive tactics can give traffickers "strong psychological power" [33, p. 10] over survivors, in addition to creating logistical challenges for a survivor trying to exit a trafficking situation.

It is important to note that the definitions of human trafficking and survivor status are not always clear-cut. This is in part because survivors may cyclically exit and re-enter the trafficking "life," with potentially more than one trafficker. Thus, there may not be a definitive temporal "end" of their experience or clear notion of when a survivor is "out" of trafficking. Survivors may also not recognize the relationship as exploitative, particularly when the trafficker is a family member or intimate partner—a view that may or may not evolve with time [14]. In some cases, traffickers also coerce survivors into activities that constitute trafficking of *other* survivors, causing self-identified survivors to be labeled as traffickers. Henderson et al. termed this the "victim-offender" overlap [59].

In the United States, certain groups are more vulnerable to being trafficked, including people of color and Indigenous people, people in poverty, undocumented immigrants, and people with a history of trauma [108]. Traffickers frequently leverage these identities to manipulate or control survivors, e.g., by threatening to report an undocumented survivor to immigration authorities [101]. Bailey and Shayan argued that the high rate of sex trafficking among Indigenous women and girls[1] is, in part, a product of "the intergenerational impacts of colonialism" [7, p. 130] including poverty, high rates of violence, isolation, misogyny, and racism.

2.2 Sex Trafficking and Sex Work

Although this study looks at all kinds of human trafficking, we must specifically position sex trafficking within the broader context of sex work. Sex work exists on a spectrum, ranging from survivors of trafficking to consensual sex workers who have full autonomy [16]. Some consensual sex workers are also survivors of sex trafficking [49].

Unfortunately, it is common among anti-trafficking efforts to treat all sex work as trafficked sex work [13, 44, 62, 67, 70, 77, 87, 92]. Bandyopadhyay et al. argue, "The most persistent of all trafficking myths asserts that the destination of all trafficking is prostitution, all prostitutes are women, and as no woman can deliberately choose to be a prostitute, all of them are trafficked" [8, p. 104]. Anti-trafficking advocates sometimes justify the "rescue" of consensual sex workers under the guise that they simply don't realize they are being trafficked [13, 44, 49, 67].

The conflation of sex work and sex trafficking obscures the true prevalence of sex trafficking. Many reports on human trafficking overestimate prevalence by including consensual sex work in their measurements, while others are "based largely on supposition and estimates" [13, p. 316]. In most countries, sex work is criminalized, making it more difficult to accurately measure sex trafficking apart from sex work [93]. Inflated statistics lead to increased policing of sex workers and, as a result, still more sex workers being mislabled as trafficking survivors [67, 87].

Worse, treating all sex work as sex trafficking directly harms sex workers. Efforts to identify trafficking survivors often mislabel consensual sex workers [62], reducing sex worker wellbeing [2, 98] and leading to increased violence, deportation, and arrest [44, 62]. The introduction of FOSTA/SESTA [97]—U.S. legislation that holds online platforms liable for hosting content that aids trafficking—has deplatformed sex workers and compromised their access to resources they rely on to find work and maintain their safety [10, 18, 20, 31, 62, 89]. Although FOSTA/SESTA is U.S. law, it has impacted sex workers globally [10, 137]. And on top of harming sex workers, legislation targeting platforms does not solve trafficking, either: Thakor and boyd wonder, "if the average person can now get Craigslist and say 'No one's being sold on Craigslist therefore no one's being sold,' did we, in fact, do a disservice to working on this issue?" [130, p. 278].

With this context in mind, we remind the reader that this study is focused on human trafficking, not consensual sex work. Sex workers do face technology-faciliated attacks, but their primary adversaries are their clients, their audience, and the state (expanded upon in § 2.4). In contrast, this study is concerned with the threats that survivors of sex and labor trafficking face from *traffickers*—a very different, highly-motivated adversary known to use strong coercive tactics.

2.3 Technology and Human Trafficking

As social, economic, and labor infrastructures are increasingly digitized, so is human trafficking.

Recruitment and exploitation. One major area of work examines traffickers' use of technology for recruitment and exploitation. Research has shown that recruitment increasingly occurs online [100]: traffickers post fraudulent job ads [3, 35, 114] or reach out to potential victims through social media and dating platforms [3, 7, 35, 46, 75, 76, 136]. That said, Gezinski and Gonzalez-Pons [51] point out that empirical evidence measuring online recruiting is limited, making it hard to accurately assess prevalence.

Traffickers also use technology as means of commercial exploitation, to advertise forced labor [3, 76, 135, 136], communicate with buyers [7, 76, 135, 136], and facilitate monetary transactions [35, 95, 96]. Thorn found that when survivors are younger, it is more likely that the trafficker is communicating with buyers on their behalf [136]. "Remote interactive sexual acts" [99, p. 58] over video calls, messages, or social media are some of the most common forms of sex work, trafficked or not [35, 56, 95, 99]. In labor trafficking, survivors may also be forced to use technologies to engage in identity theft, data fraud, and online scams [94, 96]. Meanwhile, as traffickers use technology to facilitate their exploitation, they also leverage sophisticated technology to anonymize themselves [115].

Disrupting trafficking. Technology-based efforts to disrupt trafficking have also received significant attention. Knowing the ways traffickers use technology, prior work developed data analytics

[1]This is one part of the crisis known as MMIWG (Missing and Murdered Indigenous Women and Girls).

tools that attempt to algorithmically identify and investigate trafficking [28, 74, 96, 102, 132, 136]. For example, these tools involve analyzing sex work advertisements and online interactions for signs of exploitation [74, 102, 136], attempting to identify survivors based on images created during trafficking [96], and using blockchain to make supply chains more transparent [28]. In a more survivor-engaged approach, Thinyane and Bhat [132] built an app called Apprise that facilitates screening interviews with migrant workers, enabling frontline service providers to better communicate with the workers and identify if they may be experiencing trafficking. Technology has also been used to educate the public about trafficking [1, 86, 94] and to help at-risk populations like migrant workers crowdsource information about exploitative organizations [3, 30, 94, 96].

Although this line of work has received much attention, some technological "solutions" to trafficking have been criticized as inaccurate [41, 65], privacy-violating [40], and generally unethical [17, 22, 96]. For example, as previously discussed, technology-assisted methods to identify survivors of trafficking often mislabel and cause harm to consensual sex workers [62]. Automated identification methods also fuel moral panics, such as the myth that large sporting events such as the Super Bowl are a hub for trafficking [80]. As an alternative strategy, Gezinski and Gonzalez-Pons recommend tackling structural risk factors rather than the online platforms traffickers sometimes use [51].

Technology-facilitated control. Although the prior work in this area is rich, little research has investigated *survivors'* experiences with technology, both within the trafficking situation and as a tool to aid recovery. A 2023 Forbes article reported that a popular family tracking app, Life360, is often cited in federal investigations as a tool used to control survivors of sex trafficking [24]. Bouché and Shady [21] showed how traffickers carefully monitor and control survivors' access to their technological devices, focusing on how traffickers decide the level of access to grant different survivors. A 2019 report by the UN identifies the potential for technology to "help traffickers control and coerce victims" [66, p. 2], citing possible examples such as "smart" devices that monitor exploited domestic workers, or explicit digital images that traffickers use to blackmail and control survivors of sex trafficking, but does not describe the extent or nature of their use in practice. Harassment, too, could occur over technology, since technology already facilitates communication between survivors and traffickers [114].

Two works from Chen et al. [33] and Thorn [136] are most related to our study. Chen et al. [33] interviewed victim service providers to understand the role of technology in their interactions with trafficking survivors. They found that support workers regularly grapple with technology-facilitated monitoring of their clients, indicating that more work is needed to understand the monitoring that survivors face during trafficking. Thorn, in 2018, surveyed 260 survivors of domestic minor sex trafficking to inform technology-related interventions [136]. They found that while most respondents had access to their own cell phone during their trafficking experience, over half said their trafficker had purchased the device, and half of the respondents reported that their use of technology was monitored. Based on their findings, they argue "it is important to continuously review how technology is used by traffickers, victims, and buyers" [136, p. 10].

These works indicate that traffickers use technology as a tool for monitoring and control. However, their findings do not tell the whole story. Chen et al. [33] focused on victim service providers' strategies, not survivors' experiences of technology-facilitated coercive control. Thorn [136] did focus on technological control, but they only include one subset of trafficking survivors (youth who faced sex trafficking) and their findings introduce more questions (e.g., what methods do traffickers use to "listen on their calls" [136, p. 35]?). Thus, to this literature, we contribute a qualitative study that investigates how trafficking survivors experience technology-facilitated coercive control, the impact of technology on survivors' attempts to attain digital safety and security, and the design of potential interventions to aid survivors' recovery.

2.4 Techology Safety for Survivors of Digital Violence

Outside of trafficking contexts, a growing body of work examines technology-facilitated abuse with survivors of digital violence [12, 144]. Perhaps most closely related, researchers have investigated technology-facilitated abuse in intimate partner violence (IPV). Cuomo et al. [38] used the term to "technology-enabled coercive control" to highlight the role technology plays in coercive dynamics in IPV. Freed et al. [47] and Matthews et al. [82] investigated how abusers use technology in IPV, including how domestic abusers frequently re-purpose legitimate apps like family tracking apps for abusive purposes. Tseng et al. [138] uncovered the tools and tactics abusers use for intimate partner surveillance, while Bellini et al. [11] showed how abusers justify this surveillance in online forums. Ceccio et al. [29] and Stephenson et al. [124, 125] explored how smart technologies are used as tools of control in domestic violence, while Henry et al. [60] and Eaton et al. [43] positioned image-based sexual abuse as a tool of coercive control in IPV.

Trafficking and IPV share some similarities; as noted above, many traffickers may be an intimate partner, spouse, or family member of the survivor [14]. However, no prior work has explicitly investigated (i) the extent to which technology-facilitated abuse in trafficking contexts may parallel IPV contexts or (ii) technology-enabled coercive tactics that may be unique to human trafficking.

Similarly, sex trafficking survivors may share digital safety concerns with consensual sex workers. In contrast to trafficking survivors, who face abuse by a trafficker, the primary adversaries for consensual sex workers are clients/audience members and the state. Prior work has found that sex workers, especially those with an online presence [56], face digital threats including stalking [27, 56], rampant harassment [27, 68, 122], and mass surveillance from platforms and law enforcement [87, 118]. Sex workers' content may be stolen [10, 68, 122] and information about them shared publicly [27, 68]. More broadly, sex workers are systematically deplatformed and discriminated against online, even on non-sex-work related accounts [6, 16, 19, 83, 123, 128], resulting in a loss of community and support [5], financial instability [122, 123], feelings of powerlessness [5], and a loss of digital tools that support safe work conditions [18, 20, 31]. It is likely that sex trafficking survivors face

Table 1: Participating Advocates and Survivors – Summary of the 21 advocates and survivors we interviewed. The advocates have varied expertise in whether they serve survivors of sex trafficking, survivors of non-sexual labor trafficking, youth survivors, and survivors during the trafficking situation. Participants with IDs SA# or S# have lived experience of trafficking. Table 2 gives more information about the organizations participants worked for.

				Advocacy Expertise			
ID	**Org.**	**Current Role**	**Years Exp.**	Sex trf.	Labor trf.	Youth	During
A1	Org3	Case management	1	♦	♦	♦	♦
A2	Org13	Legal advocacy	18	♦	♦		
A3	Org5	Legal advocacy	10	♦			
A4	Org13	Legal advocacy	3	♦	♦		
A5	Org10	Legal advocacy	1	♦			♦
A6	Org10	Mental health; Case management	8	♦			♦
A7	Org8	Mental health	2	♦		♦	♦
A8	Org9	Outreach	2	♦	♦		♦
A9	Org12	Program leadership; Law enforcement	19	♦	♦		♦
A10	Org11	Program leadership	14	♦	♦		
A11	Org2	Program leadership	11	♦	♦		
A12	Org5	Program leadership	10	♦	♦	♦	♦
A13	Org7	Program leadership	7	♦		♦	♦
A14	Org6	Program leadership	5	♦	♦		♦
A15	Org14	Sustaining progress	10	♦	♦	♦	
A16	Org3	Sustaining progress	4	♦	♦		
SA1	Org6	Case management	9	♦			♦
SA2	Org4	Case management; Sustaining progress	3	♦			♦
SA3	Org1	Shelter coordination	4	♦	♦		♦
S1	–	Survivor	–	–	–	–	–
S2	–	Survivor	–	–	–	–	–

some or all of these challenges, too, in addition to any technology abuse by the trafficker.

Prior research has also examined how survivors of violence seek help for technology concerns [55, 88], particularly in IPV. For example, Zou et al. [145] investigated customer support services' interactions with IPV survivors, while Freed et al. [48] and Slupska et al. [120] explored digital safety practices of gender-based violence advocates. A cluster of papers has studied the creation and deployment of computer security clinics for IPV survivors [39, 57, 139, 140]. In these models, professional IPV advocates are able to refer survivors they work with to a technology abuse clinic where technologists trained in the dynamics of IPV help the survivor navigate their digital privacy and security concerns.

However, to date, these technology abuse clinics have only served survivors of IPV. There is a need to explore if and how these models may be expanded to help survivors of technology-facilitated abuse in other contexts, including human trafficking. Doing so safely, and in ways that respect the nuances and complexities of trafficking contexts, will first require a deep understanding of trafficking survivors' experiences with technology that our paper aims to provide.

3 Methods

We contribute a qualitative study consisting of semi-structured interviews with trafficking survivors and advocates who support them. Trafficking survivors can draw from their lived experience, sharing the types of tech abuse they faced, their strategies for staying safe, and the types of services that might have been useful in their situation. At the same time, advocates have a unique perspective, not only understanding the experiences of survivors they serve, but also the strategies and services used by their clients.

3.1 Interview Procedures

Recruitment. We advertised the study via email to staff at advocacy organizations that serve trafficking survivors. The recruitment email explained that we were interested in studying the role of technology in human trafficking, with the goal of informing the design of new services for survivors. We specified that we were seeking to interview (1) people who provided support to survivors of sex and labor trafficking, and (2) people with lived experience of trafficking who were in a safe situation and who had any kind of technology-related concerns during their experience. We also used snowball sampling, reaching out to organizations and specific people whom the advocates suggested. All participants were offered a US $25 gift card for their time.

Participants. In total, we interviewed 21 participants (Table 1): 16 advocates (A1–A16), 3 survivor-advocates with lived experience of trafficking (SA1–SA3), and 2 survivors (S1 & S2). Our advocate participants came from three U.S. states (primarily New York and Wisconsin) and one national U.S. organization.[2] They have a combined 141 years of experience in the field, and include program

[2]We did not specifically exclude participants or organizations outside the U.S., but none turned up during snowball sampling.

Table 2: Organizations – The advocates we interviewed come from 14 organizations. Most organizations are victim service providers serving trafficking survivors and survivors of other types of gender-based violence. A few advocates come from broader anti-trafficking organizations, legal aid providers, and a youth independent living program.

			Stated Focus Areas				
Org ID	**U.S. State**	**Type**	Trafficking	IPV	SV	GBV	Youth
Org1	WI	Victim service provider	♦	♦	♦		♦
Org2	NY	Victim service provider	♦	♦	♦		
Org3	NY	Victim service provider	♦				
Org4	WA	Victim service provider	♦				
Org5	NY	Victim service provider	◊	♦		♦	
Org6	WI	Victim service provider	◊		♦		
Org7	WI	Victim service provider	◊				♦
Org8	WI	Victim service provider	◊				♦
Org9	WI	Victim service provider		♦	♦		
Org10	WI	Victim service provider		♦			
Org11	WI	Victim service provider		♦			
Org12	National	Broad anti-trafficking organization	◊		♦		♦
Org13	NY	Legal aid	♦	♦		♦	
Org14	WI	Youth independent living program					♦

◊ = Specifically serves sex trafficking survivors, not labor trafficking.
IPV = Intimate partner violence; SV = Sexual violence; GBV = Gender-based violence

leaders, case managers, outreach specialists, shelter coordinators, legal advocates, mental health professionals, and people helping survivors sustain progress (e.g., job placement specialists). All advocates have served survivors of sex trafficking and 12 have also served survivors of non-sexual labor trafficking. Five advocates have served youth survivors. Of the advocates, 12 have helped survivors who were still being trafficked, while 7 have only served survivors who have attained some distance from the situation.

In addition to three advocates who self-identified as survivors, we interviewed two more survivors of trafficking, S1 and S2. To protect these participants' privacy, we avoided collecting any information about the survivors beyond the interview data. The survivors did not explicitly label the type of trafficking they faced and thus we do not classify their experiences here.

Organizations included. The advocates come from 14 organizations (Table 2), mostly victim service providers (VSPs) for survivors of trafficking, IPV, sexual violence, or gender-based violence. Aside from VSPs, advocates worked for a broad anti-trafficking organization, a legal aid service, and an independent living program for at-risk youth.

We specifically did *not* exclude advocates from organizations adversarial to sex work. Thus, we must note that 2 of the 14 organizations (accounting for 3 of the 19 advocates interviewed) employ practices known to be harmful to sex workers. The stated goal of Org6 is to address both sex trafficking and local prostitution, while Org12 employs automated methods to support law enforcement in identifying trafficking, a practice known to harm sex workers [2, 44, 62, 98].

Although we do not condone these organizations' practices, we believe it important to understand the perspectives of their advocates to answer our research questions and, in turn, improve on the status quo. For one, these services do work with trafficking survivors, so excluding sex-work-adversarial organizations would risk a skewed representation of how tech abuse arises and is addressed in trafficking—in the worst case, erasing the experiences of the survivors who receive services from these organizations. Furthermore, is clear that any technology service for trafficking survivors will need to, at least in the near term, operate in an ecosystem that includes organizations adversarial to sex work. Engaging with advocates from these organizations can help us understand how to avoid practices harmful to consensual sex workers. Finally, we note that while we disagree with their organizations' practices, we appreciate how the staff and clients of these organizations offered their time and energy (and, in the case of SA1, risk of re-traumatization) to share their insights based on their lived experiences.

To avoid causing any harm by including these organizations, we took care to engage critically with their contributions. We also do not report on any discussion of harmful practices that had no direct bearing on our research questions; these types of harmful practices are already well-documented in prior work [2, 44, 62, 98].

Procedures. All interviews were held over Zoom and conducted by the first author between July and September 2024. At the start of each interview, the interviewer read an oral consent script to the participant and asked for their verbal consent to participate. They also asked for the participant's consent to record the interview; all participants agreed.

Interviews with advocates began with introductory questions about their current role and experience providing services to trafficking survivors. Then, the interviewer asked about the roles of technology in trafficking and the experiences and concerns their clients have raised about technology. Finally, the interviewer asked

how advocates and their clients manage technology concerns and what interventions or services might help.

Interviews with survivors followed a similar structure. The interviewer began with an introduction and establishing rapport with the survivor. Then, they asked the survivor to describe their experience and any technology-related experiences or concerns that were involved. They inquired about the survivor's biggest safety priorities and concerns—technological and otherwise—during their experience, and how they found support for those concerns (if they did). Finally, the interviewer asked about the survivor's perception and use of technology today. For survivor-advocate interviews, we used a hybrid of the two procedures, focusing primarily on the survivor-advocate's lived experience. The procedures are provided in the Appendix.

3.2 Qualitative Data Analysis

We analyzed the interview data following Kuckartz's three-stage process for qualitative data analysis [72]. Our process involved (i) structural coding of high-level categories, (ii) inductive generation of subcodes within these categories, and (iii) identification of themes within and across categories.

Data preparation. Immediately following each interview, we generated a transcript using NoScribe, an open-source, locally-run tool [69]. The first author cleaned each transcript by listening to the recording, correcting errors, and redacting any potentially identifying or unique information (including names, organizations, locations, and dates). With a transcript ready, we destroyed the audio recording.

High-level structural coding. To begin analysis, the first author generated a set of structural codes based on our research questions and interview procedures. These fell into two broad groups: categories about how technology is involved in human trafficking (RQ1 and RQ2) and categories related to current or proposed interventions (RQ3). After the authors met to discuss and approve these structural codes, the first author applied the structural codes to all interview transcripts.

Thematic analysis. The first and second authors (*the coders*) then used Braun & Clarke's thematic analysis [23] to generate themes from the data. We used collaborative qualitative analysis (CQA) [109] to ensure consistency by reaching agreement throughout the coding process.

To begin, the coders selected an initial set of three interviews and analyzed the interviews separately, creating individual codebooks. The coders met to discuss, create a shared codebook, and re-code the interviews using the shared codebook. Next, each coder separately applied the codebook to four more interviews. We met again to discuss any differences, update the codebook if needed (although we did not need to add any new codes), and reconcile our codes for the four transcripts. Finally, the coders evenly divided the remaining 14 interviews for analysis. For each interview, one person was the primary coder, who applied the codebook; the other was a secondary coder, who reviewed the coding and raised disagreements or concerns if applicable. The final codebooks are provided as an Appendix. Finally, having become intimately familiar with the data, the coders clustered related codes into seven overarching themes that represent our data. The resulting themes from this process are shown in Table 3.

Positionality. The authors' backgrounds and experiences impact our research, including our interpretation of the qualitative data [9, 15]. The authors are technologists and researchers with extensive experience working with survivors of technology-facilitated interpersonal abuse and gender-based violence. However, the authors have less experience in the human trafficking space; therefore, we sought advice and input from trafficking experts and professional advocates when crafting study procedures and before deploying them. Additionally, all authors believe that sex work is work and assert that not all sex work is trafficked.

During analysis, the coders reflexively incorporated their professional experiences working with survivors of abuse and drew on critical frameworks rooted in trauma-informed, survivor-centered, and anti-oppressive ethics. This includes acknowledging the physical, emotional, and behavioral impacts of trauma [142], recognizing survivors as experts of their own experiences [34], and understanding that human trafficking is intertwined with colonial and patriarchal histories (especially slavery) that are inseparable from survivors' intersectional social and political identities [36, 37, 73, 131].

3.3 Ethical Considerations

In this IRB-approved study, we took steps to protect participants' privacy. The only identifying information we kept about participants was their email address, to provide compensation and share the results of the work with participants; emails and the associated participant IDs were stored separate from study data. All transcripts were scrubbed of potentially identifying or unique information before storage. In addition, this paper was thoroughly reviewed to ensure that the quotes and anecdotes we share are sufficiently general and that we do not share confidential safety tactics used by survivors or consensual sex workers.

To support participants' wellbeing, we assured them that they could pause or stop the interview or the recording at any time, with no impact to their compensation. The interviewer has experience interviewing and interacting with survivors of gender-based violence, and conducted survivor interviews with care and compassion. The questions were scoped to focus on research-relevant topics. Before starting interviews, we shared our protocols with a trafficking advocate to ensure clarity and avoid triggering or controversial language. The researchers maintained a list of support services and resources in case a survivor became distressed or upset.

Finally, we acknowledge that working in this space can take a toll on researchers. The graphic nature of some interviews was difficult at times during interviewing and coding. The research team is trained in trauma-informed care, which includes practices for self care to mitigate vicarious trauma, and we took steps to protect our wellbeing when needed. For example, we redacted graphic portions of the interviews, took breaks from the work as needed, and sought support from each other when challenges arose.

4 Technology as a Means of Control and Tool for Resistance

We organize our findings into three parts (Table 3) that correspond to our three research questions. In this section, focused on RQ1,

Table 3: Summary of Findings – An outline of our three findings sections and themes captured within them.

Section		Theme	
§ 4	Technology as a Means of Control and Tool for Resistance	§ 4.1	Traffickers use technology to surveil, blackmail, threaten, impersonate, and harass survivors.
		§ 4.2	Survivors creatively evade cybersurveillance and use technology to connect with support services, albeit with some risks.
§ 5	Navigating Longer-Term Recovery	§ 5.1	Traffickers try to find and contact survivors, threatening their safety and their peace of mind.
		§ 5.2	Digital records, such as archived images and articles, have long-lasting impacts on survivor's ability to heal and thrive.
		§ 5.3	Those safety concerns (§ 5.1) and digital records (§ 5.2) create challenges for survivors' economic mobility.
§ 6	Imagining Technology-Related Interventions	§ 6.1	Participants, with some caveats, would value context-sensitive services addressing threat mitigation and technology literacy.
		§ 6.2	Survivors would also benefit from structural support, such as policy changes on technology platforms and broader cultural shifts.

we discuss the types of technology-facilitated coercive control that came up in our interviews, as well as how survivors use technology as a means of resistance and help-seeking during the trafficking experience. Section 5, focused on RQ2, then analyzes the role of technology in survivors' longer-term recovery as they work to attain lasting digital safety and security. Finally, Section 6, focused on RQ3, explores potential interventions and support services that might help trafficking survivors.

Note to readers. The following three sections contain accounts of trafficking and abuse that may be difficult to read. Specifically, this section mentions sexual violence, threats of violence, (redacted) obscenity, and degrading language.

4.1 Technology-Enabled Coercive Control in Human Trafficking

Traffickers use technology to convince survivors that they cannot escape undetected, that they would face dire consequences if they attempted to do so, and that they would have nowhere to go should they succeed. We provide a detailed account of these tactics.

Surveillance. One of the most common coercive tactics used by traffickers is technology-enabled surveillance, in which traffickers monitor survivors' behaviors, electronic communications, or location. Location tracking in particular is "*the biggest thing that affects our folks*" (A6), and multiple participants reported that traffickers frequently utilize *dual-use* technologies [32]: mainstream technologies with legitimate purposes that are repurposed for abuse, such as GPS trackers, social media, apps like Apple FindMy, and AirTags. Workplace surveillance through digital or "smart" cameras creates a feeling that "*the boss [trafficker] could always potentially be watching*" (A4), particularly in labor trafficking scenarios such as massage parlors, domestic servitude, and trafficking done by diplomats [58]. Outside of workplace surveillance, traffickers use basic technology, such as phone calls, to create surveillance tethers. A13 recalls meeting with survivors who were apparently alone but who "*look like they're on the phone with someone during our conversations.*"

In contrast to prior work on intimate partner violence [29], we find that surveillance is often overt: traffickers explicitly inform survivors of real or alleged monitoring as a tool for manipulation, or use physical access to coerce survivors into handing over their devices or accounts, simply demanding "*Give me your phone, I'll go through it*" (SA1). Nonetheless, survivors often maintain access or seeming ownership of their devices, which may lead to a false sense of security. They may think "*I'm not being trafficked. I have my phone, I have everything*" (A10)—but all along, "*the trafficker's monitoring their usage*" (A14). Especially when the trafficker is an intimate partner, this access may be freely given, viewed as "*initially being okay*" (A10), since digital sharing is common in intimate relationships [81]. However, seemingly "caring" actions from an intimate partner or employer, like being given a credit card, belie the fact that the trafficker "*can check, any time, any movement of that credit card*" (A8). Survivors navigating cultural differences, being less familiar with U.S. technical infrastructure, were particularly vulnerable to these tactics.

Blackmail and threats. The second most frequently cited form of technology-enabled coercion during trafficking was the use of blackmail and threats. For example, access to devices is withheld as "*a source of punishment*" or granted as a reward "*if you provide a sexual favor, if you behave or follow rules*" (A10). Non-citizen survivors, whose traffickers frequently hold their identity documents, are especially vulnerable to being cut off from their support systems because, as A8 explained, if "*you don't have an ID or passport, you can't get a phone line.*"

Technology also enables traffickers to extend their reach into survivors' social circles and triangulate family members and loved ones, even across borders. In labor trafficking, traffickers often explicitly threaten "*the safety and well being of [survivors'] family*

members, children, parents...people who they love and their support system" (A10). For youth who met traffickers over social media, digital directories and people-search websites allowed traffickers to look up personal details to underscore threats. Traffickers targeting youth online might demand, "*Send me a nude picture or else I will hurt your family,*" followed by a message "*sharing the family's address and family's phone number*" (A13). At the same time, some traffickers were "*wise not to put threats into texts*" as an intentional maneuver around laws that could incriminate them for coercion.

In sex trafficking, threats tended to center on reputational harm via image-based sexual abuse (IBSA). Like in intimate partner violence, where IBSA is frequently used as a deliberate tactic to exert "temporal control" [38] through intimidation, entrapment, and degradation [38, 43, 60], IBSA was a pattern recurrent in our interviews. Traffickers procure explicit visual media by covertly filming consensual acts, eliciting media via threats, or filming sexual assault and rape. Once obtained, traffickers might "*threaten to post them if we talked or if we left*" (SA3), sometimes disseminating them anyway, with or without the survivor's knowledge. Although dissemination often occurrs on public platforms, many participants emphasized that distribution is often targeted to maximize reputational harms, often singling out the survivor's support system, such as parents, friends, or even children.

Impersonation. Traffickers use their access and control to survivor's devices for incriminating activities, especially when survivors are being tasked with activities that risked criminal prosecution (e.g., prostitution, drug trafficking, or money laundering). For example, SA1 described realizing that a trafficker who had access to their email had sent messages to potential buyers but "*it wasn't me sending those messages,*" and SA3 recalls a trafficker "*had posted these images, or ads, for me to be able to go out and be an escort.*" As A12 explained, traffickers "*set up accounts so that it looks like the phone line is under the victim's name*" to evade accountability. Although impersonation also occurs in, e.g., IPV, traffickers' digital trails carry the implicit or explicit threat of arrest, incarceration, and other harms inherent to the penal system.

Harassment. Finally, advocates and survivors alike described how traffickers used technology to inundate and overwhelm survivors, leaving them feeling unable to escape or interfering with their ability to use their phone. A14 recalled traffickers "*calling the phone so many times that it's unusable because it's ringing so much,*" sometimes enlisting other traffickers or even other survivors to engage in harassment: "*Even if a survivor is able to block one specific phone number, there's still other people that might be reaching out to them*" (A14). Another advocate recalls a youth survivor in a session who was scrolling through "*literally...like hundreds and hundreds of notifications and unread messages*" (A13).

Technology also allows traffickers to harass survivors nearly constantly. A9 described a trafficker who, when waiting to receive a monetary transaction, would begin sending unrelenting abusive messages "*within five minutes. Whether or not he was actually out there, he would just be like, 'B*tch, where the f*ck is my money?'*" or even texting degrading messages from outside the door as the survivor was engaging in sex work.

The bombardment and unrelenting nature of harassment can impact a survivor's ability to function, creating "*a lot of busyness and chaos in their mind that you become used to and don't know how to operate without*" (A13). The cumulative effect is "*the psychological piece that wears people down, all the texts, all the calls, all the abuse*" (A14), keeping survivors who are thinking about separating themselves from actually doing so.

4.2 Mitigation and Help-Seeking

In the face of this abuse, survivors show incredible resilience, working with advocates to creatively use technology to evade, counter, and resist coercive control. We now catalog these strategies and their potential pitfalls.

Accessing services. Support providers consistently pointed to the increased flexibility that technology provides to connect survivors with support systems, including trafficking services and social networks. As A12 put it, technology "*assists someone in figuring out a path to leaving that life and leaving the situation—if in doing that you are not exposing your plan and putting yourself in more harm's way.*" To take full advantage of this, support providers offer flexible communication methods such as hotlines, text lines, and even social media. For example, A7 recalls a youth who had disappeared mid-service ultimately reconnecting with the advocate via the agency's Facebook page, accessed at the public library.

Recognizing the potential dangers of cybersurveillance, advocates "*automatically do some technology safety planning*" (A6) as soon as a survivor reaches out, asking about safe communication methods for email or text messages. Although many advocates feel unprepared to investigate device safety, others examine devices and accounts, looking to "*see if the iPhones are connected or things like that. Basic stuff*" (A8). For advocates who seek to help their clients secure their technology, Google is often the only resource. However, some advocates have also made use of resources designed for intimate partner violence. For example, A10 has used the National Network to End Domestic Violence's technology safety website [90], and A8 has previously referred clients to an IPV tech clinic.

Evading surveillance. Ideally, survivors know which technologies of theirs are under the trafficker's control and can rely on alternatives. For example, SA3 "*actually had two phones...for me to talk to my family or friends without him knowing.*" However, in the absence of safe devices, survivors and advocates work within surveillance by avoiding raising suspicions. For instance, instead of removing sources of cyberstalking, "*we'll just be really cautious about where we're going*" (A13). In potentially compromised communications, survivors and advocates sometimes use safe words or code phrases (also noted in Chen et al. [33]) to signal, for example, "*there's someone else in the room with me reading my texts*" (A7).

However, evasive tactics can create challenges for accessing support services, especially when survivors opt to avoid any use of technology they fear is compromised. Some shelters support this approach by putting any potentially compromised phone in Faraday bags so that "*even if it's turned on, it can't be tracked*" (A2). If survivors feel there is no way to secure the device, they may "*end up ditching that phone completely*" (A6). This strategy, while effective, comes at the cost of frequent support service interruptions, as survivors repeatedly replace their contact methods whenever they suspect compromise. From advocates' perspectives, "*all of a sudden [the survivor] has a new phone number, and you are calling*

the last one, and oh, well, it's disconnected" (A16). Even if advocates can provide a clean phone for survivors, their past experiences may make them too fearful to use it: "*There is this part of paranoia where they're like, I can't even talk to you from other people's phones because that phone is hacked too*" (A8).

Combating isolation. Lastly, technology can be a powerful tool for connecting survivors with "*access to resources, support systems, accurate information*" (A10), even if that wasn't in the form of trafficking-specific support services. Especially for survivors who were not aware that they might be being trafficked and thus did not explicitly seek trafficking-related support, the Internet provides unprecedented educational opportunities for recognizing trafficking, "*like if you Google what's going to happen if your boyfriend takes your phone from you*" (A8). By connecting survivors to support systems, technology also scaffolds collective action. These community-driven strategies can be "*really creative and resilient,*" as A13 shared, citing a group of youths who share reconnaissance information about a shared trafficker in a group chat: "*This person is not getting away with anything if this group chat has anything to say about it.*"

5 Navigating Longer-Term Recovery

When survivors are in recovery, technology can still connect them to the trafficker and the trafficking experience more broadly. These lingering ties impact survivors' long-term safety, digital autonomy, and economic mobility, as we detail.

Note to readers. This section discusses coercion, harassment, and image-based sexual abuse.

5.1 Cutting Contact

If traffickers are able to find and contact survivors online, they can weaponize technology-enabled coercive tactics such as those described in Section 4.1 to reel survivors back in. A1 recalls a sex trafficking survivor who moved, but remained "*in contact with [the trafficker] through social media or phone calls, text messages.*" Survivors who are in the early stages of recovery, "*depending on where they're at, are very vulnerable to getting roped back in*" (A14). This can be an especially poignant concern for youth—so much so that, "*the court [will] order a young person to not have access to technology because it's so dangerous for their mental health and their physical safety*" (A7). Traffickers' pursuit can be relentless given their financial incentive to re-recruit survivors, in contrast to other abusers such as intimate partners.

Evading traffickers can be non-trivial when technology offers so many ways to re-connect. Should a survivor want to keep an existing phone number, blocking the trafficker's number is ineffective when "*all they have to do is kick up a new VoIP*" (A9). Even when imprisoned, traffickers are "*calling them from jail,*" and if law enforcement intervenes, "*then they'll use somebody else's account*" (A14).[3] Changing phone numbers alone may be inadequate, as survivors can still be found via "*an old WhatsApp number or an old Facebook or something*" (A14). Moreover, obtaining new devices or phone lines may be not be financially feasible for survivors who "*probably can't afford to get a new one*" (A1).

Thus, some survivors feel that the only safe option is to "*delete everything, because it just feels easier*" (A7). But total avoidance is a blunt instrument, one that risks isolating survivors from the very support systems that are a protective factor from further exploitation. Survivors create social media accounts to "*connect with friends or family from the past, [but] then the traffickers find them on social media*" (A6). SA2 remembers a survivor who wanted to use social media to track down their child, also a survivor, but "*cannot make any type of social media account because they're scared of being found.*" For foreign-born survivors using, e.g., WeChat or WhatsApp to stay connected to support systems abroad, deletion would be tantamount to giving up "*their main source of communication*" (A4). Moreover, as A14 argues, survivors "*shouldn't have to go completely off the grid just to find safety and healing.*"

Indeed, many participants observed that the inescapable contact disrupts survivor's ability to heal, sustaining their trauma, threatening their peace of mind, and preventing survivors from feeling that they've truly left. As A14 described, "*even if they're not going to engage, just having to see that message from that person is traumatizing within itself.*" A11 echoed this, explaining that when survivors see any form of digital contact, "*they just relive their experience again, essentially.*" A1 likewise described it as "*like a chain*" that can't be cut, explaining that survivors live with the constant fear that "*with the phone, they will know where I am, they will track my email...it does have an imprint in their daily life.*"

5.2 Scrubbing Digital Footprints

Adding to the adversarial threat posed by traffickers, survivors in recovery must also contend with lingering digital traces of their trafficking experiences. Chen et al. [33], for example, identified social connections to other survivors as "environmental triggers" in digital spaces. While some digital environmental triggers are indelible, other digital artifacts continue to exist online due to platforms' or possessors' refusals to remove or destroy them.

Most notably, image-based sexual abuse materials (cf. Section 4.1) haunt survivors indefinitely. SA2 recalls a jarring incident in which "*somebody contacted me and was like, Hey, I just saw you on Pornhub. And I was like, what do you mean?...Sure as heck I was on Pornhub multiple times, and I had zero idea.*" Should law enforcement retain IBSA materials as evidence, ensuing requests from survivors to reclaim and destroy them may go ignored, as SA1 learned: "*All these years later, I still wonder what happened to those pictures. Were they destroyed? Are they in a cloud somewhere? Are they in a database with the police department? I still don't know.*" Other examples of lingering media include digitally archived news stories and online accounts, such as OnlyFans, Instagram, or Facebook, that remain under the trafficker's control, all of which may contain damaging posts or information.

Survivors who want platforms to take down content related to their abuse are provided with limited options: ask the platform directly, force the platform via legal recourse, or use mediation tools built to remove explicit content. Asking platforms to remove content is often painfully fruitless, as platforms profit from trafficking survivors' continued exploitation by either passively ignoring

[3] In some prisons, incarcerated people can communicate with people on the outside using devices preloaded with messaging apps [121].

or willfully denying requests to take down abusive material. For example, when SA2 asked PornHub to remove the abusive videos, PornHub responded that "*they won't because I'm not the person that posted it. I'm like, but I'm the person in the video and this was not consensual.*" Legal injunctions prove more effective, but, as A2 argues, gatekeeping takedown requests behind lengthy or confusing legal processes means that "*that's going to be like 1% [of survivors] who can actually get that done.*"

Mediation tools, lacking both transparency and the teeth of enforcement, can "*seem scary because, well, how reliable is it? And because the trust has already been broken down so much from the trafficker*" (A7). Moreover, these tools are extremely limited; TakeItDown [45], the most frequently cited of these tools, only supports requests for individuals younger than 18. StopNCII.org [126], the only corollary for adults, has fewer participating platforms and requires the survivor to possess the media they wish to be taken down, which is often not the case in trafficking. With such ineffectual responses from platforms, survivors sometimes have more success if they "*call on their community*" (A7), organizing campaigns to report abusive content.

However valiant their efforts, survivors are often left with both unshakeable stigmatization and the betrayal of knocking on so many closed doors. Of the videos on PornHub, SA2 stated, "*I don't even know if it's still on there. I don't know how long it'll stay on there. I have no idea.*" The persistence of digital content forces survivors to continuously brace for potential ramifications, as SA1 voiced, speaking of the photos held by law enforcement: "*I would hate, in 20 years, for my kids see a picture like that.*" For youth, whose earliest digital records are mired in their trafficking experiences, the effects can be socially catastrophic "*if their friend or whatever at school Googles their name...because there's so much public evidence*" (A7). While many survivors (like SA2) decouple from their digital record by changing their names, options that allow survivors to reclaim their digital autonomy are important for survivors like S1, who finds empowerment in keeping their identity: "*I use my real name now. I used to use fake names, but no. I decided, no, I'm not going to be hiding in plain sight. I'm tired of hiding, because in a way, I'm still giving them power over me. And I can't do that anymore. They have no control over me anymore. I don't want to hide.*"

5.3 Economic Mobility: Working to Recovery

Since trafficking is fundamentally tied to labor exploitation, a key component of recovery is establishing financial security through non-exploitative labor. However, the lasting effects of trafficking can impede survivors' abilities to earn a living. For example, traffickers regularly use their access to survivor's accounts to cause financial harm, such as stealing their benefits. As another example, survivors whose digital presence includes damaging information related to their abuse may suffer from decreased employability. For non-citizens, those archives could jeopardize their work authorization. According to A2, visa applications increasingly require a sanitized digital identity, with immigration advocates advising survivors to "*close down their accounts or scrub it of everything.*"

Yet the most commonly-reported barrier to economic recovery was a lack of accessible, trauma-informed resources to help survivors transition into an increasingly digitized economy. For jobs that do not require using technology, survivors still need to overcome obstacles during the job application process itself. For example, to apply for jobs "*you need to create an account, like Workday,*" or at a minimum, provide a communication method so the job can "*contact them to make an offer*" (A16). Survivors who fear being found by a trafficker may be reluctant to create accounts or provide a contact method—justifiably so, as job application sites often sell and publish user data [104].

Moreover, many jobs require technical skillsets such as writing emails or word processing. A16 described this requirement as a major barrier, estimating that "*more than half of our clients...don't know how to use Microsoft Word.*" This was an issue for both U.S.- and foreign-born survivors. For U.S.-born survivors, education and workforce training could be disrupted either directly by the traffickers, by trafficking-related incarceration, or by socioeconomic status prior to the trafficking. S1, for example, was formerly incarcerated—a regrettably common experience for survivors of trafficking[4]—and took advantage of prison education programs that taught "*how to do Office, Word, Excel, PowerPoint and all that.*" Foreign-born survivors faced additional challenges due to cultural differences, such as differences in digital financial infrastructure. As a result, several advocates pointed to gaps in available workforce literacy programs that made them inaccessible to survivors.

Finally, when survivors do establish their own businesses, they find that advice around how to use the Internet for economic opportunities is often insensitive to their lived experiences. S2, who owns a business, was connected with a coach to help grow their business. But when the coach suggested S2 run webinars or use technology for "*promotion, marketing, advertising,*" S2 had to explain their discomfort connecting with unvetted strangers on the Internet: "*I don't want that. That terrifies me...that limits my opportunity to make money, but I don't think the coach gets it.*"

6 Imagining Technology-Related Interventions

Throughout our interviews, participants offered thoughtful insights on potential interventions that might aid survivors. We broadly classify these interventions into *support services*, staffed by trained individuals who interact directly with survivors, and *structural support*, such as tools, laws, and policies that shift the status quo in ways reflective of trafficking survivors' experiences. We note that a repeated theme voiced by participants was the desire for intentionally overlapping techniques to address the same concerns, granting survivors the autonomy to choose which option felt most fitting and comfortable for them.

6.1 Direct Survivor Support

When considering the desirability of a third-party service that specifically helps survivors navigate technology-related concerns, advocates were careful to consider the inherent drawbacks to referring clients to a new service. Advocates were especially conscious of the logistical and emotional burden placed on survivors as they were asked to navigate increasing numbers of services. Having already worked to establish trust and rapport with a survivor, they

[4]To illustrate the point, consider the Survivors of Trafficking Attaining Relief Together (START) Act in New York State, which vacates criminal convictions for trafficking survivors [91]—an act which is useful only because of the high rate of incrimination among trafficking survivors.

were aware that their clients "*are going to be incredibly slow to trust other people and share information with them*" (SA1). Importantly, A12 and A5 both pointed out that many survivors of sex trafficking have strong (or even strict) preferences for working with female-presenting support workers, which may create both logistic and perceptual challenges to establishing rapport, given technology's reputation as a male-dominated field.

Moreover, advocates emphasized the potential burdens incurred by those who offer services to trafficking survivors. When receiving services, trafficking survivors often share visceral details of the abuse they have faced. As one advocate said in our interviews, technologists who offer help should "*be equipped internally, personally, to probably see and hear some really hard things*" (A13). Indeed, although our research team has extensive experience hearing accounts of interpersonal abuse, the very graphic descriptions of exploitation we encountered in this study go beyond what we have been exposed to working in other contexts.

Taking these challenges into account, advocates identified a need and desire for two types of technology-focused support services. First, advocates wanted access to a service that assists with detecting location-tracking, securing communications, and evading contact from traffickers. Even when advocates felt comfortable helping their clients with these concerns on their own, they still saw benefit in a service that might provide extra assurance, especially when survivors suspected that a trafficker had access to their information but couldn't prove it. However, advocates cautioned that, in explicitly seeking to reduce traffickers' control over survivors, such a service would be fundamentally adversarial in nature and services would need to work on protecting the service from infiltration by traffickers. As A6 explained, "*What might end up happening is, you're going to help them with all these things. And then they're going to turn around and be able to tell their traffickers, 'Hey, here are the things that we need to look out for now.' And that would be a concern.*" Participants voiced potential ways such a service might be protected, such as by being closed to the public, with access restricted to vetted referrals from trusted services. At the same time, restricting access to the service may exclude people who need technology-focused service but don't identify as trafficking survivors, including survivors who do not see their situation as exploitative [14] or consensual sex workers [77].

Second, advocates pointed to the need for services that provide survivors with options for trauma-informed, basic technology literacy classes. Such services should be inclusive of trafficking survivors' experiences, but might benefit a broad audience who have experienced trauma around technology without necessarily requiring that people identify as a survivor of trafficking. Desired topics included scam detection, including services to help youth who "*don't have the discernment in their minds yet to know what's safe and what's unsafe*" (A1); how to protect and control personal information from appearing online; and workforce training courses.

6.2 Structural Support: Tools, Laws, & Attitudes

However, support services can only offer survivors assistance to the extent that existing tools and policies allow, and advocates and survivors made ample suggestions for missing structural support. Both advocates and survivors expressed frustration with systems that were not even open to hearing survivors' technology concerns, regardless of whether they could be addressed; SA3 would hope to be served by "*somebody who maybe like, believes me. [laughs] Because I feel like that comes up—like, 'This isn't a thing.' And then you just feel like an idiot.*" Relatedly, sex trafficking survivors, especially youth, desperately want "*a tech service that was able to immediately remove things and they could go to sleep at night*" (A7). Yet this would require policy changes on the part of technology platforms, either through voluntary cooperation or through mandated removal laws. In some cases, this would require major platforms to allow survivors to recover accounts that were in the control of traffickers, or as in SA1's case, transparency and accountability mechanisms for images retained by law enforcement. Sorely needed, this was also the most ambitious request, likely requiring a collaborative advocacy push by technologists, survivors, trafficking experts, and legal activists.

Repeatedly, advocates voiced a broad desire for resources that could empower them to help survivors directly, without the friction of referring to another service. This included tools like "*a device that would like let me be able to like see, OK, is there an AirTag in this person's car or in their stuff? I wish something like that existed*" (A6). A13 believed advocates would benefit "*from a very foundational kind of [technology safety] 101: Here are practical things that you as an advocate can do in that room,*" with A7 concurring "*We need to be educated specifically about the different kinds of things that [advocates] can encounter, the different kinds of apps, the different tactics that could be used.*"

7 Discussion

Findings from our interviews with 21 participants, including five people with lived experience of trafficking, shed light on the roles technology plays in human trafficking. We show that technology is not only a vector for coercive control and a tether connecting survivors to the trafficking experience, but also a valuable source of support, information, and connection that supports survivors' recovery. We now situate our findings within the broader literature on technology-facilitated abuse by drawing comparisons between the coercive control tactics present in human trafficking and similar tactics used by abusers in other contexts, especially IPV and consensual sex work. Then, informed by our results and these comparisons, we discuss implications for the design of services, interventions, and broader advocacy to support trafficking survivors.

7.1 Comparisons with Technology-Facilitated Coercive Control in Other Contexts

At a high level, many of the types of technology-facilitated coercive control we identified are similar to abuse tactics discussed in research on digital violence in other contexts. Most closely, we see broad overlaps with the types of attacks used by intimate abusers as taxonomized by Freed et al. [47]. For example, we saw tactics that fall within each of the four categories of attacks they defined: ownership-based access, account/device compromise, harmful messages or posts, and exposure of private information [47]. These similarities are perhaps expected, given that human trafficking frequently overlaps with IPV [14]. Location tracking, a particularly salient concern in trafficking, has also been cited in several other

adversarial contexts, including IPV [29] but also parental monitoring [52] and stalking [26]. Additionally, like traffickers, intimate abusers [47] and perpetrators of romance scams or pig butchering schemes [116] use social and emotional coercion to manipulate their victims into staying or providing access to devices and accounts.

While trafficking survivors face threats from traffickers, consensual sex workers face some similar threats, but from different adversaries. Sex workers, too, contend with rampant harassment [27, 68, 122], stalking [27, 56], and image-based sexual abuse [10, 27, 68, 122]. Digital footprints may harm sex workers when their image or information is re-used in ways they did not agree to [10, 68, 122]. And like trafficking survivors, consensual sex workers have concerns about losing access to platforms they rely on—although this concern is due to systemic deplatforming [6, 16, 19, 83, 123, 128] rather than a trafficker controlling or surveilling digital assets.

Our findings also highlight concerns about workplace surveillance within labor trafficking, a topic that has been discussed in non-trafficked work contexts. Prior work has examined surveillance in the context of domestic workers [119] and truck drivers [78]. Similarly, there are clear tensions between the owners of potentially surveilling devices and bystanders, especially when there is a power dynamic between the two parties [79, 119, 124, 125] (e.g., an employer-employee relationship).

More broadly, online harassment has been documented as a pervasive problem affecting not only IPV survivors and sex workers, but also content creators [134], journalists [143], youth [61], and many other internet users [133]. In particular, image-based sexual abuse (using real or synthetic media [25, 141]) has become a grave concern for women and others online [103]. Although some tools such as TakeItDown exist to combat varied forms of harassment, mitigations remain insufficient [134]. Our study provides yet another indication that online harassment requires urgent attention.

Nuances that differentiate trafficking from other contexts. In light of these similarities, it is important to consider what differentiates technology-facilitated coercion in trafficking contexts. Notably, we find evidence that overt surveillance is more common in trafficking than in other contexts. Traffickers want survivors to be able to move around to perform labor, while keeping them tethered via surveillance. By contrast, in contexts like IPV, perpetrators are often motivated by mistrust, suspicions of infidelity, or relational dynamics of control that encourage covert surveillance [11, 138]. Less intimate adversaries such as stalkers also rely more on covert surveillance to avoid detection [113].

Moreover, our findings suggest that traffickers are often fully aware that what they are doing is illegal. Traffickers read human trafficking statutes and act in ways that avoid incriminating themselves, often actively employing strategies that instead incriminate survivors. In addition, crowdsourced harassment is perhaps uniquely prevalent in human trafficking due to its involvement of criminal activity enacted by syndicates of traffickers. While organized group harassment happens in other contexts like internet mobs [134], trafficking appears unique in that other trafficked persons may also be recruited into harassing a survivor.

Technology-facilitated coercion in trafficking may also be disproportionately severe, encompassing vulgar and ceaseless harassment, image-based sexual abuse (with images sometimes depicting forced or coerced sex acts), and ubiquitous, overt surveillance via both technological and physical monitoring. Such extreme abuse has lasting effects on survivors and their digital lives. Although the *means* of technology-facilitated abuse may be similar to other contexts, *the abuse itself* has a different textural quality in the context of trafficking, with heightened potential for vicarious trauma and other harmful effects to support providers.

Caveats. Naturally, there are limitations to these comparisons. As previously mentioned, human trafficking encompasses a wide variety of very different types of exploitative labor relationships. The concerns and needs of survivors can vary greatly depending on their specific situation. In particular, labor trafficking is undersampled in our study; the dynamics, practices, and prevalence of technology-facilitated coercion may be different for some forms of labor trafficking, particularly where traffickers leverage survivors' vulnerabilities related to employment and immigration. Youth trafficking may also have different dynamics; for example, advocates shared a greater emphasis on prevention and technology literacy efforts for youth. Future work is needed to more deeply examine the contextual nuances impacting young survivors of trafficking.

7.2 Implications for Service Design and Technology Advocacy

One goal of our study was to investigate the extent to which services that have been created to help survivors of technology-facilitated abuse in other contexts might be adapted to help trafficking survivors. In particular, as discussed in Section 2.4, technology abuse clinics [32, 39, 57, 140] employ a model in which trained technologists meet with IPV survivors to offer personalized help navigating technology abuse. The similarities in the coercive control tactics seen in prior literature on IPV and in our study on human trafficking are encouraging because they suggest that, with appropriate care, existing technology abuse clinics may be effective channels for serving survivors of technology-facilitated abuse in trafficking contexts. Indeed, the general consensus among advocates we interviewed was that a tech-clinic-like service could be immensely useful to their clients. Such a service could fill an important need voiced by advocates in our study, who often felt ill-equipped to handle technology-related concerns themselves or who felt that survivors may benefit from additional assurances.

That said, advocates in our study raised concerns that technology abuse clinics would need to navigate carefully if they expand their services to trafficking contexts. For example, although existing technology services can help identify sources of surveillance, such as scanning for malicious apps or investigating account security settings for indications of compromise [57, 140], they *cannot* currently address issues like blackmail related to image-based sexual abuse, a salient and highly emotional concern for trafficking survivors. To avoid adding to survivors' trauma by having them re-live harmful experiences when seeking help, only be to disappointed, it will be extremely important that trauma-informed services clearly advertise and communicate their limitations [105].

As in other contexts, a deep understanding of the dynamics specific to trafficking will also be necessary to prevent causing unintentional harm. For example, as mentioned, trafficking survivors

might not feel safe receiving services from a male-presenting support worker; thus, service providers should be transparent about who will be providing services and, if possible, attempt to match survivors to a female-presenting support worker if they prefer. Additionally, technologists should be cognizant that traffickers know their activities are illegal and may seek to incriminate survivors instead of themselves. Because law enforcement often seeks expertise from technologists for tasks like documenting evidence of abuse, it will be extremely important for technologists to understand this dynamic to avoid harming the very survivors they aim to help.

Finally, service providers must be aware that the spectrum of labor conditions in the sex industry is continuous, ranging from sex trafficking to consensual sex work. This includes recognizing that some survivor support organizations may be hostile to consensual sex work and carefully navigating interactions with those organizations (e.g., by not accepting referrals from such organizations, or by appropriately handling them). Moreover, tech abuse support services should be designed to accommodate consensual sex workers who seek services from anti-trafficking organizations [49, 77] and who may face different threats compared to trafficking survivors.

Call for advocacy from technologists. Although our results show promise for technology abuse clinics in the context of human trafficking, services alone are insufficient to address trafficking survivors' digital safety concerns. Technologists have a role to play in combating technology-facilitated coercive control in human trafficking by contributing to broader technology advocacy efforts. Participants in our study repeatedly called for help removing unwanted content, including IBSA, from online spaces. Technologists should join advocacy efforts for laws, policies, and platform changes that can help survivors remove information, harassing content, and IBSA. Because human trafficking is a crime that is not protected by First Amendment speech, there is an opportunity for partnerships between platforms where content is disseminated and human trafficking service providers to facilitate mandatory takedowns. Moreover, because online harassment is widespread [113, 133], this type of advocacy would be useful to survivors of many kinds of online abuse.

In addition, our findings suggest that data brokerage and the sale of information online makes everyone more vulnerable to attacks and abuse, especially youth. We heard how traffickers use personal information found online to concretize their threats to hurt a survivor's friends or family as a means of coercion. Thus, tighter restrictions on the sale of personal information could have a preventative effect for multiple types of online abuse and exploitation [85, 110].

8 Conclusion

Our qualitative study sheds light on the technology-facilitated coercive control faced by survivors of human trafficking, how survivors use technology as a means of resistance and help-seeking during the trafficking experience, and how technology is a tool for longer-term recovery as survivors work to attain lasting digital safety and security. We show important similarities in the coercive tactics employed in trafficking contexts and other interpersonal abuse settings, suggesting that existing services for helping survivors with technology abuse may be expanded to accommodate the needs of trafficking survivors—although doing so safely will require care navigating the unique nuances of trafficking contexts. We acknowledge that our small scale study is geographically limited to only a few U.S. states and does not comprehensively represent the many types of exploitative labor under the umbrella of trafficking. Nevertheless, our work provides important steps towards helping trafficking survivors combat technology-facilitated coercive control and attain digital safety and autonomy.

Acknowledgments

This work would not have been possible without the generosity of the advocates and survivors we interviewed. We appreciate the insights of our anonymous reviewers, whose feedback improved the paper. This work was funded in part by a Google Academic Research Award as well as a grant from the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice (Grant # 15POVC-23-GK-01414-NONF). The opinions, findings, and conclusions or recommendations expressed in this paper are those of the contributors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

References

[1] A21. 2025. Can You See Me? https://www.a21.org//content/can-you-see-me/grbis0 Accessed: 2024-9-9.

[2] Aziza Ahmed and Meena Seshu. 2012. "We Have the Right Not to Be 'Rescued'...": When Anti-Trafficking Programmes Undermine the Health and Well-Being of Sex Workers. *Anti-Trafficking Review* 103-2012 (1 June 2012), 149–168.

[3] Brittany Anthony. 2018. *On-Ramps, Intersections, and Exit Routes: A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking.* Technical Report. Polaris. https://polarisproject.org/wp-content/uploads/2018/08/A-Roadmap-for-Systems-and-Industries-to-Prevent-and-Disrupt-Human-Trafficking-Social-Media.pdf

[4] Apple. 2022. An update on AirTag and unwanted tracking. https://www.apple.com/newsroom/2022/02/an-update-on-airtag-and-unwanted-tracking/

[5] Carolina Are and Pam Briggs. 2023. The Emotional and Financial Impact of De-Platforming on Creators at the Margins. *Social Media + Society* 9, 1 (Jan. 2023), 1–12. doi:10.1177/20563051231155103

[6] Carolina Are and Susanna Paasonen. 2021. Sex in the Shadows of Celebrity. *Porn Studies* 8, 4 (Oct. 2021), 411–419. doi:10.1080/23268743.2021.1974311

[7] Jane Bailey and Sara Shayan. 2021. The Missing and Murdered Indigenous Women Crisis: Technological Dimensions. In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, Bailey Jane, Flynn Asher, and Henry Nicola (Eds.). Emerald Publishing Limited, Leeds, England, 125–144. https://doi.org/10.1108/978-1-83982-848-520211007

[8] Nandinee Bandyopadhyay, Swapna Gayen, Rama Debnath, Kajol Bose, Sikha Das, Geeta Das, M. Das, Manju Biswas, Pushpa Sarkar, Putul Singh, Rashoba Bibi, Rekha Mitra, and Sudipta Biswas. 2004. 'Streetwalkers Show the Way': Refraining the Debate on Trafficking from Sex Workers' Perspective. *IDS Bulletin* 35, 4 (2004), 104–111. doi:10.1111/j.1759-5436.2004.tb00162.x

[9] Shaowen Bardzell and Jeffrey Bardzell. 2011. Towards a feminist HCI methodology: Social science, feminism, and HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)* (Vancouver, BC, May 7-12, 2011). ACM, New York, NY, USA, 675–684. https://doi.org/10.1145/1978942.1979041

[10] Catherine Barwulor, Allison McDonald, Eszter Hargittai, and Elissa M. Redmiles. 2021. "Disadvantaged in the American-dominated Internet": Sex, Work, and Technology. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 563, 16 pages. doi:10.1145/3411764.3445378

[11] Rosanna Bellini, Emily Tseng, Nora McDonald, Rachel Greenstadt, Damon McCoy, Thomas Ristenpart, and Nicola Dell. 2021. "So-called privacy breeds evil": Narrative Justifications for Intimate Partner Surveillance in Online Forums. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW3, Article 210 (Jan 2021), 27 pages. doi:10.1145/3432909

[12] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L Mazurek, Dana Cuomo, Nicola Dell, and Thomas Ristenpart. 2024. SoK: Safer Digital-Safety Research Involving At-Risk Users. In *IEEE Symposium on Security and*

Privacy (S&P 2024) (San Fransisco, CA, May 19-23, 2024). IEEE, New York, NY, 635–654. https://doi.org/10.1109/SP54263.2024.00071

[13] Kathleen Ja Sook Bergquist. 2015. Criminal, Victim, or Ally? Examining the Role of Sex Workers in Addressing Minor Sex Trafficking. *Affilia* 30, 3 (Aug. 2015), 314–327. doi:10.1177/0886109915572844

[14] Sarah Bessell. 2018. Human Trafficking and Domestic Violence Fact Sheet. The Human Trafficking Legal Center. https://www.htlegalcenter.org/wp-content/uploads/Human-Trafficking-and-Domestic-Violence-Fact-Sheet.pdf

[15] Rasika Bhalerao, Vaughn Hamilton, Allison McDonald, Elissa M Redmiles, and Angelika Strohmayer. 2022. Ethical Practices for Security Research with At-Risk Populations. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (Genoa, Italy, June 6-10, 2022). IEEE, New York, NY, 546–553. http://dx.doi.org/10.1109/EuroSPW55150.2022.00065

[16] Rasika Bhalerao and Damon McCoy. 2022. An Analysis of Terms of Service and Official Policies with Respect to Sex Work. In *2022 IEEE International Symposium on Technology and Society (ISTAS)*, Vol. 1. IEEE, New York, NY, 1–14. doi:10.1109/ISTAS55053.2022.10227104

[17] Rasika Bhalerao, Nora McDonald, Hanna Barakat, Vaughn Hamilton, Damon McCoy, and Elissa Redmiles. 2022. Ethics and efficacy of unsolicited anti-trafficking SMS outreach. *Proc. ACM Hum. Comput. Interact.* 6, CSCW2 (Nov. 2022), 1–39. https://dl.acm.org/doi/10.1145/3555083

[18] Danielle Blunt and Ariel Wolf. 2020. *Erased: The Impact of FOSTA-SESTA & the Removal of Backpage.* Community Report. Hacking//Hustling. 54 pages.

[19] Danielle Blunt and Zahra Stardust. 2021. Automating Whorephobia: Sex, Technology and the Violence of Deplatforming: An Interview with Hacking//Hustling. *Porn Studies* 8, 4 (Oct. 2021), 350–366. doi:10.1080/23268743.2021.1947883

[20] Danielle Blunt and Ariel Wolf. 2020. Erased: The Impact of FOSTA-SESTA and the Removal of Backpage on Sex Workers. *Anti-Trafficking Review* 14 (April 2020), 117–121. doi:10.14197/atr.201220148

[21] Vanessa Bouché and Stephanie Shady. 2017. A Pimp's Game: A Rational Choice Approach to Understanding the Decisions of Sex Traffickers. *Women & Criminal Justice* 27, 2 (March 2017), 91–108. doi:10.1080/08974454.2016.1250701

[22] Sabra Boyd. 2023. How AI puts trafficking survivors at risk. openDemocracy. https://www.opendemocracy.net/en/beyond-trafficking-and-slavery/how-big-tech-and-ai-are-putting-trafficking-survivors-at-risk/ Accessed: 2024-6-17.

[23] Virginia Braun and Victoria Clarke. 2012. Thematic analysis. In *APA handbook of research methods in psychology, Vol 2: Research designs: Quantitative, qualitative, neuropsychological, and biological.* American Psychological Association, Washington, 57–71. http://dx.doi.org/10.1037/13620-004

[24] Thomas Brewster. 2023. Sex Traffickers Used America's Favorite Family Safety App To Control Victims. Forbes Magazine. https://www.forbes.com/sites/thomasbrewster/2023/04/06/sex-traffickers-use-parenting-apps-like-life360-to-spy-on-victims/

[25] Natalie Grace Brigham, Miranda Wei, Tadayoshi Kohno, and Elissa M. Redmiles. 2024. "Violation of my body:" Perceptions of AI-generated non-consensual (intimate) imagery. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)* (Philadelphia, PA, August 11-13, 2024). USENIX Association, Berkeley, CA, 373–392. https://www.usenix.org/conference/soups2024/presentation/brigham

[26] Albert Fox Cahn and Eva Galperin. 2021. Apple's AirTags Are a Gift to Stalkers. Wired. https://www.wired.com/story/opinion-apples-air-tags-are-a-gift-to-stalkers/

[27] Rosie Campbell, Teela Sanders, Jane Scoular, Jane Pitcher, and Stewart Cunningham. 2019. Risking Safety and Rights: Online Sex Work, Crimes and 'Blended Safety Repertoires'. *The British Journal of Sociology* 70, 4 (2019), 1539–1560. doi:10.1111/1468-4446.12493

[28] Alex Capri. 2018. How Blockchain Could Help End Modern Day Slavery In Asia's Exploitative Seafood Industry. Forbes Magazine. https://www.forbes.com/sites/alexcapri/2018/02/14/how-blockchain-could-help-end-modern-day-slavery-in-asias-exploitative-seafood-industry/

[29] Rose Ceccio, Sophie Stephenson, Varun Chadha, Danny Yuxing Huang, and Rahul Chatterjee. 2023. Sneaky Spy Devices and Defective Detectors: The Ecosystem of Intimate Partner Surveillance with Covert Devices. In *32nd USENIX Security Symposium (USENIX Security 23)* (Anaheim, CA, August 9-11, 2023). USENIX Association, Berkeley, CA, 123–140. https://www.usenix.org/conference/usenixsecurity23/presentation/ceccio

[30] Centro de los Derechos del Migrante, Inc. 2025. Contratados. https://contratados.org Accessed: 2024-6-18.

[31] Lura Chamberlain. 2019. FOSTA: A Hostile Law with a Human Cost. *Fordham Law Review* 87, 5 (April 2019), 2171.

[32] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. 2018. The Spyware Used in Intimate Partner Violence. In *2018 IEEE Symposium on Security and Privacy (SP)* (San Fransisco, CA, May 20-24, 2018). IEEE, New York, NY, 441–458. doi:10.1109/SP.2018.00061

[33] Christine Chen, Nicola Dell, and Franziska Roesner. 2019. Computer Security and Privacy in the Interactions Between Victim Service Providers and Human Trafficking Survivors. In *28th USENIX Security Symposium (USENIX Security '19)* (Santa Clara, CA, August 14-16, 2019). USENIX Association, Berkeley, CA, 89–104. https://www.usenix.org/conference/usenixsecurity19/presentation/chen

[34] Janet X. Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. 2022. Trauma-Informed Computing: Towards Safer Technology Experiences for All. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)* (New Orleans, LA, USA, April 30–May 5, 2022). ACM, New York, NY, USA, Article 544, 20 pages. doi:10.1145/3491102.3517475

[35] January Contreras and Katherine Chon. 2022. Technology's Complicated Relationship with Human Trafficking. US Administration for Children and Families. https://www.acf.hhs.gov/blog/2022/07/technologys-complicated-relationship-human-trafficking Accessed: 2024-6-6.

[36] Kimberle Crenshaw. 1989. Demarginalizing the intersection of race and sex: A black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. *Univ. Chic. Leg. Forum* 1989, 1 (1989), 8. https://chicagounbound.uchicago.edu/uclf/vol1989/iss1/8/

[37] Kimberle Crenshaw. 1991. Mapping the margins: Intersectionality, identity politics, and violence against women of color. *Stanford Law Rev.* 43, 6 (July 1991), 1241. http://dx.doi.org/10.2307/1229039

[38] Dana Cuomo and Natalie Dolci. 2021. New tools, old abuse: Technology-enabled coercive control (TECC). *Geoforum* 126 (2021), 224–232. doi:10.1016/j.geoforum.2021.08.002

[39] Dana Cuomo and Natalie Dolci. 2022. The TECC clinic: An innovative resource for mitigating technology-enabled coercive control. In *Women's Studies International Forum*, Vol. 92. Elsevier, Amsterdam, Netherlands, 102596. doi:10.1016/j.wsif.2022.102596

[40] Julia Deeb-Swihart, Alex Endert, and Amy Bruckman. 2019. Understanding Law Enforcement Strategies and Needs for Combating Human Trafficking. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. ACM, New York, NY, USA, 1–14. doi:10.1145/3290605.3300561

[41] Julia Deeb-Swihart, Alex Endert, and Amy Bruckman. 2022. Ethical Tensions in Applications of AI for Addressing Human Trafficking: A Human Rights Perspective. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2, Article 295 (Nov 2022), 29 pages. doi:10.1145/3555186

[42] Kendra Doychak and Chitra Raghavan. 2020. "No voice or vote:" Trauma-coerced attachment in victims of sex trafficking. *Journal of Human Trafficking* 6, 3 (2020), 339–357.

[43] Asia A Eaton, Sofia Noori, Amy Bonomi, Dionne P Stephens, and Tameka L Gillum. 2021. Nonconsensual porn as a form of intimate partner violence: Using the power and control wheel to understand nonconsensual porn perpetration in intimate relationships. *Trauma, violence, & abuse* 22, 5 (2021), 1140–1154. doi:10.1177/1524838020906533

[44] empower foundation. 2018. Hit & Run II: The Impact of Anti-Trafficking Policy and Practice on Sex Worker's Human Rights in Thailand. Technical Report, 142 pages. https://68738d33-e198-469a-aa34-b8ce7e1b841b.filesusr.com/ugd/ebc7c4_7b2014bb10024ab68b18d0f4e9c9db2b.pdf

[45] National Center for Missing and Exploited Children. 2025. Take It Down. https://takeitdown.ncmec.org/

[46] Diana Freed, Natalie N Bazarova, Sunny Consolvo, Eunice J Han, Patrick Gage Kelley, Kurt Thomas, and Dan Cosley. 2023. Understanding Digital-Safety Experiences of Youth in the U.S. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)* (Hamburg, Germany, April 23-28, 2023). ACM, New York, NY, USA, 1–15. https://doi.org/10.1145/3544548.3581128

[47] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)* (Montreal, QC, Canada). ACM, New York, NY, USA, 1–13. doi:10.1145/3173574.3174241

[48] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW (Dec. 2017), 1–22. https://doi.org/10.1145/3134681

[49] Freedom Network USA and the National Survivor Network. 2023. Re-Centering Sex Worker Safety in Anti-Trafficking Work: Perspectives from the Field. Technical Report. https://freedomnetworkusa.org/app/uploads/2023/10/Recentering-Sex-Worker-Safety-in-Anti-Trafficking-Work.pdf

[50] Christine Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. 2022. "Like Lesbians Walking the Perimeter": Experiences of U.S. LGBTQ+ Folks With Online Security, Safety, and Privacy Advice. In *31st USENIX Security Symposium (USENIX Security 22)* (Boston, MA, August 10-12, 2022). USENIX Association, Berkeley, CA, 305–322. https://www.usenix.org/conference/usenixsecurity22/presentation/geeng

[51] Lindsay B. Gezinski and Kwynn M. Gonzalez-Pons. 2024. Sex Trafficking and Technology: A Systematic Review of Recruitment and Exploitation. *Journal of Human Trafficking* 10, 3 (July 2024), 497–511. doi:10.1080/23322705.2022.2034378

[52] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J LaViola, Jr, and Pamela J Wisniewski. 2018. Safety vs. Surveillance: What Children Have to Say about Mobile Apps for Parental Control. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18, Paper 124)*. ACM, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3173698

[53] Scott Gleeson. 2022. Woman used an AirTag to track boyfriend, then ran over and killed him, police say. USA Today. https://www.usatoday.com/story/news/nation/2022/06/15/woman-airtag-track-boyfriend-death/7632348001/

[54] Nitesh Goyal, Leslie Park, and Lucy Vasserman. 2022. "You have to prove the threat is real": Understanding the needs of Female Journalists and Activists to Document and Report Online Harassment. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)* (New Orleans, LA, USA). ACM, New York, NY, USA, Article 242, 17 pages. doi:10.1145/3491102.3517517

[55] Naman Gupta, Kate Walsh, Sanchari Das, and Rahul Chatterjee. 2024. "I really just leaned on my community for support": Barriers, Challenges, and Coping Mechanisms Used by Survivors of Technology-Facilitated Abuse to Seek Social Support. In *33rd USENIX Security Symposium (USENIX Security 24)* (Philadelphia, PA, August 14-16, 2024). USENIX Association, Berkeley, CA, 4981–4998. https://www.usenix.org/conference/usenixsecurity24/presentation/gupta

[56] Vaughn Hamilton, Hanna Barakat, and Elissa M. Redmiles. 2022. Risk, Resilience and Reward: Impacts of Shifting to Digital Sex Work. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2 (Nov. 2022), 537:1–537:37. doi:10.1145/3555650

[57] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2019. Clinical Computer Security for Victims of Intimate Partner Violence. In *28th USENIX Security Symposium (USENIX Security 19)* (Santa Clara, CA, August 14-16, 2019). USENIX Association, Berkeley, CA, 105–122. https://www.usenix.org/conference/usenixsecurity19/presentation/havron

[58] Jason Haynes. 2023. Revisiting the relationship between human trafficking and diplomatic immunity. *Law Q. Rev.* 139, 1 (2023), 204–210. https://pure-oai.bham.ac.uk/ws/portalfiles/portal/186345794/HaynesJ2023Revisiting.pdf

[59] Angie C Henderson and Shea M Rhodes. 2023. "Got sold a dream and it turned into a nightmare": The victim-offender overlap in commercial sexual exploitation. In *The Field of Human Trafficking*. Routledge, Abingdon, Oxfordshire, UK, 33–48.

[60] Nicola Henry, Nicola Gavey, and Kelly Johnson. 2023. Image-based sexual abuse as a means of coercive control: victim-survivor experiences. *Violence Against Women* 29, 6-7 (2023), 1206–1226. doi:10.1177/10778012221114918

[61] Sameer Hinduja and Justin W Patchin. 2013. Social influences on cyberbullying behaviors among middle and high school students. *J. Youth Adolesc.* 42, 5 (May 2013), 711–722. http://dx.doi.org/10.1007/s10964-012-9902-4

[62] Victoria Holt, Emily Kenway, and Addy Berry. 2021. Sex Workers As Collateral Damage, Once Again: A Critique Of The New 'Sex Trafficking Identification Matrix' Tool. SWARM. https://www.swarmcollective.org/sex-workers-as-collateral-damage-once-again-a-critique-of-the-new-sex-trafficking-identification-matrix-tool/

[63] Elizabeth Hopper and José Hidalgo. 2006. Invisible chains: Psychological coercion of human trafficking victims. *Intercultural Hum. Rts. L. Rev.* 1 (2006), 185.

[64] The White House. 2022. Bills Signed: H.R. 7132 and S. 4524. https://www.whitehouse.gov/briefing-room/legislation/2022/12/07/bills-signed-h-r-7132-and-s-4524/

[65] Kyle Hundman, Thamme Gowda, Mayank Kejriwal, and Benedikt Boecking. 2018. Always Lurking: Understanding and Mitigating Bias in Online Human Trafficking Detection. In *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*. ACM, New York, NY, USA, 137–143. https://dl.acm.org/doi/10.1145/3278721.3278782

[66] United Nations Inter-agency Coordination Group Against Trafficking in Persons (IACT). 2019. Human Trafficking and Technology: Trends, Challenges, and Opportunities. Technical Report. https://icat.un.org/sites/g/files/tmzbdl461/files/human_trafficking_and_technology_trends_challenges_and_opportunities_web.pdf

[67] Crystal A. Jackson. 2016. Framing Sex Worker Rights: How U.S. Sex Worker Rights Activists Perceive and Respond to Mainstream Anti–Sex Trafficking Advocacy. *Sociological Perspectives* 59, 1 (March 2016), 27–45. doi:10.1177/0731121416628553

[68] Angela Jones. 2015. Sex Work in a Digital Era. *Sociology Compass* 9, 7 (2015), 558–570. doi:10.1111/soc4.12282

[69] kaixxx. 2024. NoScribe. GitHub repository. https://github.com/kaixxx/noScribe

[70] Kamala Kempadoo. 2005. From Moral Panic to Global Injustice: Changing Perspectives on Trafficking. In *Trafficking and Prostitution Reconsidered: New Perspectives on Migration, Sex Work and Human Rights*, Bandana Pattanaik, Jyoti Sanghera, and Kamala Kempadoo (Eds.). Routledge, London, UK.

[71] Kathleen Kim. 2010. The coercion of trafficked workers. *Iowa L. Rev.* 96 (2010), 409.

[72] Udo Kuckartz. 2013. Three Basic Methods of Qualitative Text Analysis. In *Qualitative Text Analysis: A Guide to Methods, Practice & Using Software*, Udo Kuckartz (Ed.). SAGE Publications Ltd, London. http://dx.doi.org/10.4135/9781446288719

[73] Shanti Kulkarni. 2019. Intersectional Trauma-Informed Intimate Partner Violence (IPV) Services: Narrowing the Gap between IPV Service Delivery and Survivor Needs. *J. Fam. Violence* 34, 1 (Jan. 2019), 55–64. https://doi.org/10.1007/s10896-018-0001-5

[74] Mark Latonero. 2011. Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds. USC Annenberg Center on Communication Leadership and Policy. https://bpb-us-w1.wpmucdn.com/sites.usc.edu/dist/e/695/files/2011/09/HumanTrafficking_FINAL.pdf

[75] Mark Latonero, Jennifer Musto, Zhaleh Boyd, Ev Boyle, Amber Bissell, Joanne Kim, and Kari Gibson. 2012. Technology and human trafficking: The rise of mobile and the diffusion of technology-facilitated trafficking. USC Annenburg Center on Communication Leadership and Policy: Research Series on Technology and Human Trafficking. https://dx.doi.org/10.2139/ssrn.2177556

[76] Mary Leary. 2014. Fighting Fire with Fire: Technology in Child Sex Trafficking. *Duke Journal of Gender Law & Policy* 21, 2 (April 2014), 289–323.

[77] Kari Lerum and Barbara G. Brents. 2016. Sociological Perspectives on Sex Work and Human Trafficking. *Sociological Perspectives* 59, 1 (March 2016), 17–26. doi:10.1177/0731121416628550

[78] Karen Levy. 2023. *Data Driven*. Princeton University Press, Princeton, NJ. http://dx.doi.org/10.1515/9780691241012

[79] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. 2020. Smart devices in Airbnbs: Considering privacy and security for both guests and hosts. *Proc. Priv. Enhancing Technol.* 2020, 2 (April 2020), 436–458. doi:10.2478/popets-2020-0035

[80] Lauren Martin and Annie Hill. 2019. Debunking the Myth of 'Super Bowl Sex Trafficking': Media Hype or Evidenced-Based Coverage. *Anti-Trafficking Review* 13 (Sept. 2019), 13–29. doi:10.14197/atr.201219132

[81] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. "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 (CHI '16)*. Association for Computing Machinery, New York, NY, USA, 5921–5932. doi:10.1145/2858036.2858051

[82] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. 2017. 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 (CHI '17)*. ACM, New York, NY, USA, 2189–2201. https://doi.org/10.1145/3025453.3025875

[83] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW (Nov. 2019), 1–23. https://doi.org/10.1145/3359174

[84] Meta. 2022. Updates to How We Protect People on Instagram From Abuse. https://about.fb.com/news/2022/10/protecting-people-on-instagram-from-abuse/ (Accessed on 09/12/2024).

[85] Shivangi Mishra. 2021. The dark industry of data brokers: Need for regulation? *International Journal of Law and Information Technology* 29, 4 (2021), 395–410. doi:10.1093/ijlit/eaab012

[86] Rachel E Moran, Stephen Prochaska, Izzi Grasso, and Isabelle Schlegel. 2023. Navigating information-seeking in conspiratorial waters: Anti-trafficking advocacy and education post QAnon. *Proc. ACM Hum. Comput. Interact.* 7, CSCW1 (April 2023), 1–27. https://dl.acm.org/doi/10.1145/3579510

[87] Ruth Morgan Thomas. 2021. *Conflation of Sex Work and Trafficking*. Written Statement: High-Level Meeting on Trafficking in Persons. NSWP Global Network of Sex Work Projects, Edinburgh, Scotland, UK.

[88] Elizabeth A Mumford, Emily F Rothman, Poulami Maitra, and Jackie Sheridan-Johnson. 2023. US young adults' professional help-seeking in response to technology-facilitated abuse. *Journal of interpersonal violence* 38, 11-12 (2023), 7063–7088. doi:10.1177/08862605221140042

[89] Jennifer Musto, Anne E. Fehrenbacher, Heidi Hoefinger, Nicola Mai, P. G. Macioti, Calum Bennachie, Calogero Giametta, and Kate D'Adamo. 2021. Anti-Trafficking in the Time of FOSTA/SESTA: Networked Moral Gentrification and Sexual Humanitarian Creep. *Social Sciences* 10, 2 (Feb. 2021), 58. doi:10.3390/socsci10020058

[90] National Network to End Domestic Violence (NNEDV). 2025. Safety Net Project. https://www.techsafety.org/

[91] NY Anti-Trafficking Network. 2021. The START Act – Expanded Criminal Record Relief for Trafficked Individuals. https://nyscasa.org/wp-content/uploads/2022/02/Service-Provider-Advisory-on-the-START-Act.pdf

[92] NSWP Global Network of Sex Work Projects. 2011. Sex Work Is Not Trafficking. Briefing Paper #03. https://www.nswp.org/sites/default/files/SW%20is%20Not%20Trafficking.pdf

[93] NSWP Global Network of Sex Work Projects. 2018. The Impact of Anti-trafficking Legislation and Initiatives on Sex Workers. Policy Brief. https://www.nswp.org/sites/default/files/impact_of_anti-trafficking_laws_pb_nswp_-_2018.pdf

[94] Department of State: Office to Monitor and Combat Trafficking in Persons. 2024. 2024 Trafficking in Persons Report. Technical Report. https://www.state.gov/reports/2024-trafficking-in-persons-report

[95] United Nations Office on Drugs and Crime. 2021. The Role of Technology in Human Trafficking. Technical Report. https://www.unodc.org/unodc/en/human-trafficking/Webstories2021/the-role-of-technology-in-human-trafficking.html Accessed: 2024-6-6.

[96] United Nations Working Group on Trafficking in Persons. 2021. Successful strategies for addressing the use of technology to facilitate trafficking in persons and to prevent and investigate trafficking in persons. Technical Report. https://www.unodc.org/documents/treaties/WG_TiP_2021/CTOC_COP_WG.4_2021_2/ctoc_cop_wg.4_2021_2_E.pdf

[97] 115th US Congress P.L. 115-64. 2018. Allow States and Victims to Fight Online Sex Trafficking Act of 2017. https://www.govinfo.gov/content/pkg/PLAW-115publ164/pdf/PLAW-115publ164.pdf

[98] Lucy Platt, Pippa Grenfell, Rebecca Meiksin, Jocelyn Elmes, Susan G. Sherman, Teela Sanders, Peninah Mwangi, and Anna-Louise Crago. 2018. Associations between Sex Work Laws and Sex Workers' Health: A Systematic Review and Meta-Analysis of Quantitative and Qualitative Studies. *PLOS Medicine* 15, 12 (Dec. 2018), e1002680. doi:10.1371/journal.pmed.1002680

[99] Polaris. 2019. The Typology of Modern Slavery. Technical Report. https://polarisproject.org/wp-content/uploads/2019/09/Polaris-Typology-of-Modern-Slavery-1.pdf Accessed: 2024-6-6.

[100] Polaris. 2022. Analysis of 2020 National Human Trafficking Hotline Data. Technical Report. https://polarisproject.org/2020-us-national-human-trafficking-hotline-statistics/ Accessed: 2024-6-6.

[101] Polaris. 2024. Human Trafficking 101. https://polarisproject.org/human-trafficking-101/ Accessed: 2024-6-3.

[102] Rebecca S Portnoff, Danny Yuxing Huang, Periwinkle Doerfler, Sadia Afroz, and Damon McCoy. 2017. Backpage and bitcoin: Uncovering human traffickers. In *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. ACM, New York, NY, USA, 1595—1604. https://dl.acm.org/doi/10.1145/3097983.3098082

[103] Lucy Qin, Vaughn Hamilton, Sharon Wang, Yigit Aydinalp, Marin Scarlett, and Elissa M. Redmiles. 2024. "Did They F***ing Consent to That?": Safer Digital Intimacy via Proactive Protection Against Image-Based Sexual Abuse. In *33rd USENIX Security Symposium (USENIX Security 24)* (Philadelphia, PA). USENIX Association, Berkeley, CA, 55–72. https://www.usenix.org/conference/usenixsecurity24/presentation/qin

[104] Edith Ramirez, Julie Brill, Maureen K Ohlhausen, Joshua D Wright, and Terrell McSweeny. 2014. Data Brokers: A Call for Transparency and Accountability. Federal Trade Commission. https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

[105] Lana Ramjit, Natalie Dolci, Francesca Rossi, Ryan Garcia, Thomas Ristenpart, and Dana Cuomo. 2024. Navigating Traumatic Stress Reactions During Computer Security Interventions. In *33rd USENIX Security Symposium (USENIX Security 24)* (Philadelphia, PA). USENIX Association, Berkeley, CA, 2011–2028. https://www.usenix.org/conference/usenixsecurity24/presentation/ramjit

[106] Jody Raphael. 2020. Parents as pimps: Survivor accounts of trafficking of children in the United States. *Dignity: A Journal of Analysis of Exploitation and Violence* 4, 4 (2020), 7. doi:10.23860/dignity.2019.04.04.07

[107] Representative Ocasio-Cortez. 2024. Rep. Ocasio-Cortez Leads Bipartisan, Bicameral Introduction of DEFIANCE Act to Combat Use of Non-Consensual, Sexually-Explicit "Deepfake" Media. Press Release. https://ocasio-cortez.house.gov/media/press-releases/rep-ocasio-cortez-leads-bipartisan-bicameral-introduction-defiance-act-combat (Accessed on 09/12/2024).

[108] Reuters. 2024. Technology and human trafficking: Fighting the good fight. https://legal.thomsonreuters.com/blog/technology-and-human-trafficking/

[109] K Andrew R Richards and Michael A Hemphill. 2018. A Practical Guide to Collaborative Qualitative Data Analysis. *J. Teach. Phys. Educ.* 37, 2 (2018), 225–231. doi:10.1123/jtpe.2017-0084

[110] Theodore Rostow. 2017. What happens when an acquaintance buys your data: A new privacy harm in the age of data brokers. *Yale J. on Reg.* 34 (2017), 667.

[111] Kevin A. Roundy, Paula Barmaimon Mendelberg, Nicola Dell, Damon McCoy, Daniel Nissani, Thomas Ristenpart, and Acar Tamersoy. 2020. The Many Kinds of Creepware Used for Interpersonal Attacks. In *2020 IEEE Symposium on Security and Privacy (SP)* (San Fransisco, CA, May 18–21, 2020). IEEE, New York, NY, 626–643. doi:10.1109/SP40000.2020.00069

[112] Pratyasha Saha, Nadira Nowsher, Ayien Utshob Baidya, Nusrat Jahan Mim, Syed Ishtiaque Ahmed, and S M Taiabul Haque. 2024. Computing and the Stigmatized: Trust, Surveillance, and Spatial Politics with the Sex Workers in Bangladesh. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24, Article 780)*. ACM, New York, NY, USA, 1–22. https://doi.org/10.1145/3613904.3642005

[113] Nithya Sambasivan, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Sanely Gaytán-Lugo, David Nemer, Elie Bursztein, Elizabeth Churchill, and Sunny Consolvo. 2019. "They Don't Leave Us Alone Anywhere We Go": Gender and Digital Abuse in South Asia. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland, UK) *(CHI '19)*. ACM, New York, NY, USA, 1–14. doi:10.1145/3290605.3300232

[114] Beth Sapiro, Laura Johnson, Judy L. Postmus, and Cassandra Simmel. 2016. Supporting Youth Involved in Domestic Minor Sex Trafficking: Divergent Perspectives on Youth Agency. *Child Abuse & Neglect* 58 (Aug. 2016), 99–110. doi:10.1016/j.chiabu.2016.06.019

[115] Siddhartha Sarkar. 2015. Use of Technology in Human Trafficking Networks and Sexual Exploitation: A Cross-Sectional Multi-Country Study. *Transnational Social Review* 5, 1 (Jan. 2015), 55–68. doi:10.1080/21931674.2014.991184

[116] Jason Scharfman. 2024. Crypto romance scams and pig butchering. In *The Cryptocurrency and Digital Asset Fraud Casebook, Volume II*. Springer Nature Switzerland, Cham, 39–63. http://dx.doi.org/10.1007/978-3-031-60836-0_2

[117] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. 2018. Computer Security and Privacy for Refugees in the United States. In *2018 IEEE Symposium on Security and Privacy (SP)* (San Fransisco, CA). IEEE, New York, NY, 409–423. http://dx.doi.org/10.1109/SP.2018.00023

[118] Aria Slippert. 2022. Platform Pimps: The Puppet Masters of the Porn-opticon. *The iJournal: Student Journal of the Faculty of Information* 7, 2 (May 2022), 43–46. doi:10.33137/ijournal.v7i2.38615

[119] Julia Slupska, Selina Cho, Marissa Begonia, Ruba Abu-Salma, Nayanatara Prakash, and Mallika Balakrishnan. 2022. "They Look at Vulnerability and Use That to Abuse You": Participatory Threat Modelling with Migrant Domestic Workers. In *31st USENIX Security Symposium (USENIX Security 22)* (Boston, MA). USENIX Association, Berkeley, CA, 323–340. https://www.usenix.org/conference/usenixsecurity22/presentation/slupska-vulnerability

[120] Julia Slupska and Angelika Strohmayer. 2022. Networks of Care: Tech Abuse Advocates' Digital Security Practices. In *31st USENIX Security Symposium (USENIX Security 22)* (Boston, MA). USENIX Association, Berkeley, CA, 341–358. https://www.usenix.org/conference/usenixsecurity22/presentation/slupska-networks

[121] Phillip Vance Smith, II. 2023. My Girlfriend and I Used to Rely on Weekly Letters to Communicate. Then, "Texting" Came to My Prison. Slate. https://slate.com/technology/2023/12/e-messaging-prison-gettingout-romantic-relationships.html Accessed: 2024-9-9.

[122] Ananta Soneji, Vaughn Hamilton, Adam Doupé, Allison McDonald, and Elissa M. Redmiles. 2024. "I feel physically safe but not politically safe": Understanding the Digital Threats and Safety Practices of OnlyFans Creators. In *33rd USENIX Security Symposium (USENIX Security 24)* (Philadelphia, PA). USENIX Association, Berkeley, CA, 1–18. https://www.usenix.org/conference/usenixsecurity24/presentation/soneji

[123] Zahra Stardust, Danielle Blunt, Gabriella Garcia, Lorelei Lee, Kate D'Adamo, and Rachel Kuo. 2023. High Risk Hustling: Payment Processors, Sexual Proxies, and Discrimination by Design. *CUNY L. Rev.* 26 (2023), 57.

[124] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, and Rahul Chatterjee. 2023. "It's the Equivalent of Feeling Like You're in Jail": Lessons from Firsthand and Secondhand Accounts of IoT-Enabled Intimate Partner Abuse. In *32nd USENIX Security Symposium (USENIX Security 23)* (Anaheim, CA). USENIX Association, Berkeley, CA, 105–122. https://www.usenix.org/conference/usenixsecurity23/presentation/stephenson-lessons

[125] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, Danny Yuxing Huang, and Rahul Chatterjee. 2023. Abuse Vectors: A Framework for Conceptualizing IoT-Enabled Interpersonal Abuse. In *32nd USENIX Security Symposium (USENIX Security 23)* (Anaheim, CA). USENIX Association, Berkeley, CA, 69–86. https://www.usenix.org/conference/usenixsecurity23/presentation/stephenson-vectors

[126] StopNCII.org. 2025. Stop Non-Consensual Intimate Image Abuse. https://stopncii.org/

[127] Angelika Strohmayer, Jenn Clamen, and Mary Laing. 2019. Technologies for Social Justice: Lessons from Sex Workers on the Front Lines. In *CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–14. doi:10.1145/3290605.3300882

[128] #SurvivorsAgainstSESTA. 2025. Platforms Which Discriminate Against Sex Workers. https://survivorsagainstsesta.org/platforms-discriminate-against-sex-workers/

[129] Leonie Maria Tanczer, Isabel López-Neira, and Simon Parkin. 2021. 'I feel like we're really behind the game': perspectives of the United Kingdom's intimate partner violence support sector on the rise of technology-facilitated abuse. *Journal of Gender-Based Violence* 5, 3 (2021), 431–450. http://dx.doi.org/10.1332/239868021x16290304343529

[130] Mitali Thakor and danah boyd. 2013. Networked Trafficking: Reflections on Technology and the Anti-Trafficking Movement. *Dialectical Anthropology* 37, 2 (June 2013), 277–290. doi:10.1007/s10624-012-9286-6

[131] The Combahee River Collective. 1986. *Combahee River Collective Statement: Black Feminist Organizing in the Seventies and Eighties*. Kitchen Table: Women of Color Press, Albany, NY, USA.

[132] Hannah Thinyane and Karthik S Bhat. 2019. Apprise: Supporting the Critical-Agency of Victims of Human Trafficking in Thailand. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19, Paper 155)*. ACM, New York, NY, USA, 1–14. https://doi.org/10.1145/3290605.3300385

[133] Kurt Thomas, Devdatta Akhawe, Michael Bailey, Dan Boneh, Elie Bursztein, Sunny Consolvo, Nicola Dell, Zakir Durumeric, Patrick Gage Kelley, Deepak Kumar, Damon McCoy, Sarah Meiklejohn, Thomas Ristenpart, and Gianluca Stringhini. 2021. SoK: Hate, Harassment, and the Changing Landscape of Online Abuse. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, New York, NY, 247–267. http://dx.doi.org/10.1109/SP40001.2021.00028

[134] Kurt Thomas, Patrick Gage Kelley, Sunny Consolvo, Patrawat Samermit, and Elie Bursztein. 2022. "It's common and a part of being a content creator": Understanding How Creators Experience and Cope with Hate and Harassment Online. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. ACM, New York, NY, USA, Article 121, 15 pages. doi:10.1145/3491102.3501879

[135] Thorn. 2015. A Report on the Use of Technology to Recruit, Groom, and Sell Domestic Minor Sex Trafficking Victims. Technical Report. https://www.thorn.org/wp-content/uploads/2015/02/Survivor_Survey_r5.pdf

[136] Thorn. 2018. Survivor Insights: The Role of Technology in Domestic Minor Sex Trafficking. https://www.thorn.org/wp-content/uploads/2018/06/Thorn_Survivor_Insights_061118.pdf

[137] Erin Tichenor. 2020. 'I've Never Been So Exploited': The Consequences of FOSTA-SESTA in Aotearoa New Zealand. *Anti-Trafficking Review* 14 (April 2020), 99–115. doi:10.14197/atr.201220147

[138] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2020. The Tools and Tactics Used in Intimate Partner Surveillance: An Analysis of Online Infidelity Forums. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Berkeley, CA, 1893–1909. https://www.usenix.org/conference/usenixsecurity20/presentation/tseng

[139] Emily Tseng, Diana Freed, Kristen Engel, Thomas Ristenpart, and Nicola Dell. 2021. A Digital Safety Dilemma: Analysis of Computer-Mediated Computer Security Interventions for Intimate Partner Violence During COVID-19. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. ACM, New York, NY, USA, Article 71, 17 pages. doi:10.1145/3411764.3445589

[140] Emily Tseng, Mehrnaz Sabet, Rosanna Bellini, Harkiran Kaur Sodhi, Thomas Ristenpart, and Nicola Dell. 2022. Care Infrastructures for Digital Security in Intimate Partner Violence. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 123, 20 pages. doi:10.1145/3491102.3502038

[141] Rebecca Umbach, Nicola Henry, Gemma Faye Beard, and Colleen M. Berryessa. 2024. Non-Consensual Synthetic Intimate Imagery: Prevalence, Attitudes, and Knowledge in 10 Countries. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 779, 20 pages. doi:10.1145/3613904.3642382

[142] Bessel A Van der Kolk. 2015. *The Body Keeps the Score: Brain, Mind, and Body in the Healing of Trauma.* Penguin Publishing Group, New York, NY.

[143] Noel Warford, Nicholas Farber, and Michelle L. Mazurek. 2024. How Entertainment Journalists Manage Online Hate and Harassment. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)* (Philadelphia, PA). USENIX Association, Berkeley, CA, 279–295. https://www.usenix.org/conference/soups2024/presentation/warford

[144] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya Sleeper, and Kurt Thomas. 2022. SoK: A Framework for Unifying At-Risk User Research. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, New York, NY, 2344–2360. doi:10.1109/SP46214.2022.9833643

[145] Yixin Zou, Allison McDonald, Julia Narakornpichit, Nicola Dell, Thomas Ristenpart, Kevin Roundy, Florian Schaub, and Acar Tamersoy. 2021. The Role of Computer Security Customer Support in Helping Survivors of Intimate Partner Violence. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Berkeley, CA, 429–446. https://www.usenix.org/conference/usenixsecurity21/presentation/zou

A Interview Procedures for Advocates

Section 0: Introductory

- What is your current role? Briefly, what does that entail?
  - Do you serve survivors of sex trafficking, labor trafficking, or both?
  - Do you provide services to anyone other than trafficking survivors?
  - When do you intervene: mid-trafficking situation, crisis management, or sustaining progress?
- How long have you been working with survivors of trafficking?

Section 1: Tech Abuse in Trafficking

- In your experience, how often do trafficking cases involve technology?
  - To clarify: By "technology" we mean digital technologies like phones, online accounts, location-sharing services or devices, etc.
- How, if at all, do traffickers use technology to control and abuse survivors?
  - Do they monitor survivors' communications or technology use?
  - Do they surveil what survivors do offline, for example with GPS trackers?
  - Do they own or control survivors' devices and accounts?
  - Do they restrict access to devices or accounts?
  - Do they threaten to post non-consensual intimate imagery?
  - Do they impersonate or defraud survivors online?
- How, if at all, do traffickers use technology to recruit survivors?
- How, if at all, does technology facilitate forced labor?
  - For example, do traffickers advertise online, or are survivors forced to do online labor (like digital sex work)?
- How, if at all, does technology impact survivors' attempts to exit trafficking?
- How, if at all, do these experiences affect survivors' long-term relationship with technology?
- How, if at all, does the role of technology differ between sex and labor trafficking?
  - Are there certain types of trafficking where technology abuse is more common (for example, domestic labor)?
- Have you seen cases where trafficking overlapped with intimate partner or family violence?
  - What was the role of technology in that situation?

Section 2: Interventions for Tech Abuse in Trafficking

- How do you assess survivors' technology-related concerns? Is there a standard screening procedure?
  - (If yes) Can we see a copy of these procedures?
- What are survivors' primary concerns about technology?
- When survivors raise concerns about technology, what trainings, resources, or services do you turn to? Are there standard practices in place?
  - Do you offer services over Zoom or video calls? How is that impacted?
- What do survivors do to mitigate their technology concerns?
- Is there a risk that addressing technological concerns could escalate traffickers' control and abuse? In what way?
- What role, if any, does technology play in combating trafficking?

- What technology-related training materials or resources would you like to have access to?
- Which would you prefer: to help clients with their technology concerns yourself (with training and help from these resources), OR to refer clients to a separate technology-focused service? Why?
- Who would be best suited to provide technology-focused support: advocates, technologists trained in trafficking, mental health professionals trained in technology, or someone else? Why?
- What concerns would you have about directing survivors to a trained technologist to address these concerns?
  - How much information would need to be shared? Would that be an issue?
- What do you want to tell tech companies [government agencies, etc.] about their role in human trafficking?

Section 3: Feedback (early interviews only)

- We are still working to refine our interview procedures. What feedback do you have for this interview? Is there anything we should update?
- Our goal with this study is to design technology-focused services for trafficking survivors. Toward this goal, would it be beneficial for us to engage directly with survivors?
  - (If yes) What method should we use to engage with survivors? For example, focus groups/support groups, individual interviews, online surveys? Could you help us recruit survivors for this study?
  - (If no) Why not? Are there other people you think we should engage with instead?
- Who else should we talk to about this study? Can you connect us?

B Interview Procedures for Survivors

Section 0: Background *Framework for mutual learning about language:* We've done a lot of research and spoken to advocates before this, but if you have any feedback on the words, phrasing, or language I use during the interview, please feel free to point it out at any time. It's okay to interrupt me if you'd like.

- (Interviewer: Introduce myself, where I'm from, a little about me.)
- Would you like to tell me a bit about yourself? For example, where are you from?
- How would you describe your tech abilities? Do you have a technical background?
  - To clarify: By "technology" we mean digital technologies like phones, online accounts, location-sharing services or devices, etc.
- Why did you sign up for this study?
- Tell me a little bit about your experience [with trafficking].
  - Type of trafficking
  - Relationship with the perpetrator
  - Perpetrator's comfort with technology
  - Their current situation

Section 1: Experiences of Tech Abuse in Trafficking

- In what ways, if any, was technology involved in your experience?
- Was technology ever used to harass, threaten, or monitor you as part of the trafficking?
  - Were your communications or technology use monitored?
  - Were you surveilled offline, for example with GPS trackers?
  - Were your devices and accounts owned or controlled by someone else?
  - Was your access restricted to your devices or accounts?
  - Did anyone threaten to post your personal information such as intimate images?
  - Were you impersonated or defrauded online?
- Were you originally reached out to or recruited through technology? In what way?
- Were you ever made to do digital labor? For example, doing video calls?
- Were there ever ads posted about you online, by you or others, during the trafficking?

Section 2: Safety Planning & Mitigations

- When thinking about how to keep yourself safe, either when making your own plans or when talking with a support worker, what were your biggest priorities?
  - Did technology help or hinder your efforts to address these priorities? In what ways?
- Was technology included in your thinking about how to keep yourself safe? Why or why not?
  - (If yes) What were some of the considerations and risks when thinking about taking steps to safeguard your tech?
  - (If yes) Was there anything that made your tech feel safer during this time?
- In what ways is your situation now still impacted by these technology concerns? Do you still face challenges as a result?
- (If distanced) How did you end up leaving the situation?
  - In what ways was technology helpful or harmful during this time?

Section 3: Brainstorming Services

- Which people or organizations have you reached out to for support, if any?
  - Did they ask about your technology concerns?
  - What support did they give you for your technology concerns, if any?
- What services or resources would have been helpful to addressing your technology concerns?
  - Where would it have been most feasible for you to get this kind of support?
  - Would you have liked to get this help from people you already reached out to, or to have a new place to go specifically for tech concerns?
  - Who would you have preferred to get help from? For example, a tech expert, a customer support person, or a familiar caseworker?
- Looking back on this experience, is there any advice you would give people who are facing similar technology concerns? What worked or didn't work for you?

Section 4: Perception of Technology

- Nowadays, how do you use technology in your daily life?
- Do you think the trafficking experience changed how you interact with technology? Why [not]?
- What would you want to tell tech companies [+ any other entities that came up] about their role in human trafficking?
- Do you have any questions for me? Do you have any comments on the interview procedure?

C Codebooks

The codebooks generated during analysis are shown in Table 4 and Table 5.

Received 12 September 2024; revised 10 December 2024; accepted 16 January 2024

Table 4: Technology Codebook – The first half of our codebook: codes related to technology's role in human trafficking.

Code	#
Tech abuse	207
↪ Monitoring & surveillance	43
↪ Location tracking	42
↪ Blackmail & extortion	32
↪ Physical access	31
↪ Harassment & unwanted contact	25
↪ Social, romantic, & intimate relationships	25
↪ Proxy attacks/crowdsourcing	12
↪ Tampering & evidence deletion	12
↪ Immigration, citizenship, & cultural differences	11
↪ Sophisticated attacks	10
↪ Financial harm	6
Impacts	168
↪ Interferences with daily functioning	59
↪ Reachability to trafficker	43
↪ Hypervigilance & paranoia	29
↪ Loss of digital autonomy	29
↪ Institutional betrayal & grief	21
↪ Economic mobility	18
↪ Support service interruptions	14
↪ Tech avoidance	12
Differences between types of trafficking	72
Facilitation using technology	67
Recruitment using technology	55
Prevalence of tech concerns	28

Table 5: Interventions Codebook – The second half of our codebook: codes related to interventions and mitigations.

Code	#
Mitigations	253
↪ Trauma-informed security & privacy	72
↪ Support worker strategies	67
↪ Trauma-informed basic tech literacy	44
↪ Proof, evidence, & forensics	40
↪ Individual survivor actions	36
↪ Accessibility of services	33
↪ Rebuilding digital autonomy	27
↪ Establishing safe communication	24
↪ Collective survivor actions	4
Design considerations	151
↪ Sensitivity to context	55
↪ Rapport & comfort	32
↪ Trusted expert	31
↪ Autonomy & choice	29
↪ Handoff & coordination	27
↪ Staff overwhelmed	12
Desired resources	60
Assessing tech concerns	50
Tech as a positive	47
Survivors' priorities	38