Computer Security and Privacy in the Interactions Between Victim Service Providers and Human Trafficking Survivors

Christine Chen, ***University of Washington;*** **Nicola Dell,** ***Cornell Tech;*** **Franziska Roesner,** ***University of Washington***

https://www.usenix.org/conference/usenixsecurity19/presentation/chen

This paper is included in the Proceedings of the 28th USENIX Security Symposium.

August 14–16, 2019 • Santa Clara, CA, USA

978-1-939133-06-9

Open access to the Proceedings of the 28th USENIX Security Symposium is sponsored by USENIX.

Computer Security and Privacy in the Interactions Between Victim Service Providers and Human Trafficking Survivors

Christine Chen
Paul G. Allen School of Computer Science & Engineering
University of Washington

Nicola Dell
The Jacobs Institute
Cornell Tech

Franziska Roesner
Paul G. Allen School of Computer Science & Engineering
University of Washington

Abstract

A victim service provider, or VSP, is a crucial partner in a human trafficking survivor's recovery. VSPs provide or connect survivors to resources such as medical care, legal services, employment opportunities, etc. In this work, we study VSP-survivor interactions from a computer security and privacy perspective. Through 17 semi-structured interviews with staff members at VSPs and survivors of trafficking, we surface the role technology plays in VSP-survivor interactions as well as related computer security and privacy concerns and mitigations. Our results highlight various tensions that VSPs must balance, including building trust with their clients (often by giving them as much autonomy as possible) while attempting to guide their use of technology to mitigate risks around revictimization. We conclude with concrete recommendations for computer security and privacy technologists who wish to partner with VSPs to support and empower trafficking survivors.

1 Introduction

Human trafficking is a crime in which a perpetrator, or "trafficker", preys on vulnerable individuals through atrocities such as sexual exploitation, forced labor, or the removal of organs [30]. As a conservative estimate, around 24.9 million individuals worldwide are being exploited in this manner [16]. Technology is playing an increasing role in this ecosystem, from enabling trafficking via online platforms (e.g., [2, 18]) to aiding in the detection and halting of trafficking (e.g., [6, 25]).

In this work, we focus on a previously understudied role that technology plays in the human trafficking ecosystem: technology in the interactions between trafficking survivors and organizations known as victim service providers, or VSPs. VSPs exist to support their clients by providing resources such as temporary shelter, help with employment and legal issues, and mental health support. In this work, we focus on VSPs providing resources to individuals who are exiting or recovering from a trafficking situation. These resources are critical in protecting these individuals from former or future exploiters ("revictimization").

Our research is driven by the following questions: How do VSPs communicate and interact with their clients (trafficking survivors), and, particularly, what role does technology play in that interaction? What are VSPs' computer security concerns and threat models, both for themselves and on behalf of their clients? What technical (or non-technical) strategies do they use to mitigate these concerns? And, ultimately, what opportunities exist to better safeguard VSPs and their clients from a computer security perspective?

To investigate these questions, we conducted a qualitative interview study with 17 participants, including staff members at VSPs and several trafficking survivors. We analyzed these interviews using thematic analysis common in qualitative research. Our findings shed light on the general role of technology in VSP-survivor interactions (Section 4.1), the computer security concerns and threat models of VSPs and their clients (Section 4.2), and the corresponding defenses, where present (Section 4.3). We identify fundamental tensions and challenges that must be taken into account by technologists who wish to improve VSP and client security and privacy (Section 5).

At a high level, we find that VSPs make technology-related choices with the goals of protecting their clients from revictimization and other harm. Specific instances of how VSPs protect clients include helping clients lock down social media accounts and enforcing shelter rules restricting photos or social media posts (that may reveal the shelter's location). We also find that, sometimes, the most effective means for VSPs and their clients to interact are not the most conducive to client safety. For example, despite the potential risk of trafficker-compromised accounts, some VSPs use Facebook to communicate with clients because it provides a reliable way to reach them even in the absence of cellular service. More generally, we find that our participants must balance building client trust and maintaining contact with imposing technology-related client safety rules.

From findings such as these, we distill concrete recom-

mendations for those in the computer security and privacy community, and for technologists at large, wishing to help support survivor-VSP relationships. For example, we provide guidelines on securing communications in situations when the client's device is compromised by an adversary with physical access and raise awareness around the threat posed to survivors by publicly available information (e.g., public records) online. In investigating the interactions between survivors of human trafficking and VSPs from a computer security and privacy perspective, our work contributes to the larger push to leverage technology for good in the fight against human trafficking.

2 Background and Related Work

There is a growing body of research examining the role of technology in both facilitating and fighting human trafficking (e.g., [2, 12, 17–19, 24]). In the computer science community in particular, prior work has developed technology to aid investigators in examining online sex ads and online forums for trafficking activity [6, 25].

Focusing on the victim service provider ecosystem, there has been research that explores the ways anti-trafficking organizations utilize technology to collaborate with each other [29] as well as efforts within the VSP community to leverage technology in providing help to trafficking victims [20]. Work outside of the technical realm has examined how survivors of trafficking [4] or domestic violence [13] experience and react to the assistance provided by VSPs.

Beyond human trafficking, the computer security and privacy community has studied other specific (often at-risk) populations, including journalists [22], refugees [28], and undocumented immigrants [14]. Most relevant to our work is research studying computer security and privacy for survivors of intimate partner violence [5, 10, 11, 21]. Where relevant, we highlight similarities between our findings with these prior studies on related populations.

In this work, we focus on an aspect of the human trafficking ecosystem that has not been rigorously studied from an academic, technical perspective: the interactions *between* VSPs and trafficking survivors. We ask, from a computer security and privacy perspective: how does technology enable or hinder these relationships, and how do VSPs and their clients consider and mitigate the potential technology-related risks that may undermine the survivor's path to recovery?

3 Methodology

Between March and July 2018, we conducted 17 semi-structured interviews with staff members at victim service provider organizations and several trafficking survivors.

Recruitment. Recruitment took place through several primary methods: introductions facilitated by community members and anti-trafficking leaders, the authors' personal connections, and snowball sampling. Our recruitment advertisements specified that we were looking for advocates who work with labor trafficking and/or sex trafficking survivors to speak about how they use technology in their work. We also specified that participants would be compensated $30.

Participants. Table 1 provides an overview of the 17 study participants. The 17 participants represented 11 different organizations; survivors P14 and P17 were not affiliated with a specific organization at the time of the study. 16 participants were based in the U.S. and one participant was based in a Southeast Asian country. Most participants were based in urban areas.

As Table 1 shows, most participants currently focus on serving survivors of sex trafficking (though some participants may have previously helped labor trafficking survivors as well). To avoid confusion, we do our best throughout this paper to call out results that are specific to interactions with labor trafficking survivors or sex trafficking survivors. Finally, to be clear, note that some of the participants who focus on sex trafficking survivors naturally also serve individuals in the sex trade who may not technically fall within the parameters of sex trafficking (e.g. individuals who claim to be in the sex trade voluntarily).

Study Protocol. The interviews ran between 60-90 minutes. We began with groundwork questions to understand the participant's role in supporting clients and general thoughts on technology's influence on the trafficking ecosystem. We then asked questions that would help surface how VSPs use technology in their interactions with clients and what, if any, concerns exist around this technology usage. We asked about participants' experiences with technology with regards to first contact with clients, client intake, organization and client safety, and day-to-day interactions. To avoid priming participants to overemphasize their computer security and privacy concerns, most questions focused generally on technology in client-VSP interactions and related concerns but did not mention computer security and privacy in particular.

Finally, we showed participants two prototypes for secure communication (created by others): single-use URLs (a URL that leads to sensitive content, which gets changed to innocuous content when the same URL is accessed again) and disappearing messages [1, 8, 9]. Our goal was to elicit reactions and threat models using these concrete examples, not to propose these particular technologies as perfect solutions. To avoid participants giving inflated positive responses towards the tools (participant response bias), we stated these goals clearly for participants and also stated that we did not make the tools. We asked questions like: When, if at all, might you use this? How could it be helpful? How could it introduce more risk? The full interview protocol can be found in Appendix A.

ID	Job Title	Focus	Client Nationality	Client Age
P1	Advocate, Survivor Leader	Sex Trafficking	Domestic	Adult
P2	Advocate	Sex Trafficking	Domestic	Adult
P3	Director	Sex Trafficking	Domestic	All
P4	Director	Sex Trafficking	Domestic	Youth, TAY
P5	Advocate	Labor Trafficking	International	Adult
P6	Director	Sex Trafficking	Domestic	All
P7	Advocate	Sex Trafficking	Domestic	Youth, TAY
P8	Advocate	Labor and Sex Trafficking	Domestic, International	All
P9	Advocate	Sex Trafficking	Domestic	Youth, TAY
P10	Advocate, Survivor Leader	Sex Trafficking	Domestic	Youth, TAY (to 25)
P11	Advocate	Sex Trafficking	Domestic	Youth, TAY (to 30)
P12	Advocate	Labor and Sex Trafficking	International	Adult
P13	Advocate	Sex Trafficking	Domestic, International	TAY
P14	Survivor Leader	Sex Trafficking	N/A	N/A
P15	Advocate	Sex Trafficking	Domestic, International	did not disclose
P16	Director	Labor and Sex Trafficking	Domestic, International	Adult
P17	Survivor Leader	Sex Trafficking	N/A	N/A

Table 1: Summary of Participants. *Advocates* support clients one-on-one, *Directors* oversee the VSP's human trafficking services (managing advocates as well as interacting with clients), and *Survivor Leaders* are survivors of trafficking (in this case, sex trafficking) who are raising awareness and leading trainings on the issue. Transition age youth (TAY) are individuals between the ages of 16 and 24 [32]; where specified, participants also worked with clients slightly outside of this range.

Ethical Considerations. Our study was declared exempt by the University of Washington human subjects review board (IRB). We obtained informed consent from participants to conduct and (optionally) to audio record the interview. As the interviews could touch on highly sensitive topics (especially for survivors), we ensured that participants knew that they could skip questions and request a break at any time. We also emphasized that participants should provide only as much detail in their answers as they felt comfortable with. All electronic files were password protected, and physical consent forms and notes were stored in a secure location.

Data Analysis. We continued conducting interviews until no new themes emerged (saturation). We analyzed the data thematically using a common methodology for qualitative data [3]. We conducted multiple passes through the data in which we iteratively identified and clustered themes, or codes, present in the data. Two researchers independently read through transcripts of several interviews, generated an initial set of codes, met in person to develop an initial codebook, and iteratively refined this codebook by applying it to additional interviews. Once the codebook was finalized, two researchers divided up the remaining interviews and coded them. We emphasize that the nature of our data is qualitative, not quantitative, so we do not report on raw numbers of participants who made certain statements in the results.

4 Results

We now turn to our results. After providing an overview of the general practices our participants and their organizations use in interacting with trafficking survivors, we will present the security and privacy concerns and mitigation strategies — and tensions and challenges — that arise in these interactions. We use the terms "survivor" and "client" interchangeably, depending on the context and following the norms described by our participants during the interviews. At times, we also use the term "victim" and note that VSP clients may not be fully removed from a trafficking situation when they are receiving services.

4.1 Client-VSP Interactions

This section provides background and context for the more in-depth security and privacy discussions in later sections.

4.1.1 Role of VSPs

Though VSPs may help trafficking victims escape their situations, their primary role is to help clients with the many challenges they face on the path to stability, including looking for employment, applying for housing, dealing with legal matters, and coping with severe trauma. Importantly, as we investigate in this paper, VSPs protect clients and train

clients to protect themselves from revictimization into a trafficking situation.

Some of our participants work at VSPs that provide shelter for clients. These arrangements range from emergency shelters (with very low barrier to entry — e.g., a client can stay even if he or she is on drugs) to long-term homes (where the client must be committed to actively working towards goals and self-sustainability). As we discuss in Section 4.3, shelter locations are sometimes confidential to help protect clients.

As an overarching challenge in providing services to clients, participants described the delicate balance they must walk between building trust with their clients — so that they can best advise and maintain contact with them — and doing what they believe is best for the client. As clients have left (or as they are in the process of deciding whether to leave) a situation where they have had little control over their lives, participants often talked about how crucial it is to give clients as much autonomy as possible. For example, P13 talked about working with clients who want to find a job. While she would like her clients to go to school, she does not force her idea of what would be best on the client. Throughout out results, we will see this tension recur in the context of technology-related guidelines and choices that VSPs are hesitant to push on their clients.

4.1.2 First Contact

Clients typically make their first contact with VSPs through referrals — e.g., from law enforcement, schools, or other VSPs — or via a phone hotline. Hotlines may receive emergency calls, playing a similar role to 9-1-1 for clients and trafficking victims. For example, P7 described answering hotline calls from individuals who are running for their lives at the moment, and P8 talked about how they will dispatch a Lyft or Uber to a caller who has just escaped.

Dispersal and discovery of hotline numbers happens in a variety of ways. Beyond relying on word of mouth (a common method), participants talked about posters with the hotline number placed in public locations such as hospitals, train stations, and rest stops. One organization has their hotline number on a local Spanish TV channel. Another mode of dispersal is through personal items (e.g., soap, essential oil, hats, etc.) handed out to at-risk individuals (e.g. farm workers) with the hotline number hidden discreetly on the object.

For individuals still in trafficking situations, calling the hotline can be dangerous (if the individual is constantly being monitored by their trafficker) or even impossible (if the individual does not have a device). In these situations, participants described the ingenuity of their clients in finding ways to access technology to get help. For example, one of P16's labor trafficking clients saved up enough money from tips to buy a burner phone from a gas station. While the burner phone did not have the capability to connect to the Internet, he had seen a hotline number earlier and committed it to memory. As another example:

> P8: I've had a few clients who, in escaping... [were] able to get access to a hidden phone or discretely (on an app that their trafficker isn't aware...is a messaging app)...send messages to a friend who helps them get help...

From advocates who work with sex trafficking survivors, we heard how clients will search the web for help:

> P2: We've had a couple people. I'm like, "How did you learn about us?" She goes, "I googled prostitutes [city]."

At the same time, participants worried that lack of technical expertise could make it challenging for clients to find help online. For example:

> P1: I think what people have a hard time with is search words. I think people don't understand how Google works, and how to search for things.

Mention of direct outreach by VSPs to potential clients was rare, but one participant uses the phone numbers in online sex ads to conduct text message campaigns to contact individuals who might want help leaving. Another participant, P3, said that her organization reaches out to people who like the organization's Facebook page to see if they need help.

4.1.3 Continued Communication

Our participants typically communicate with clients via phone calls, SMS, social media (e.g., Facebook), email, and in person. Participants generally talked of using the communication method that their clients feel most comfortable with. P16 described how digital communication can help put clients at ease.

> P16: I find that many of our clients are more comfortable engaging through technology because it's less raw. It's a step removed in some ways...

Communication methods that work over WiFi were often mentioned as important, as clients may not be able to afford reliable cellular service or even a reliable device:

> P2: A client right now has a phone. It's not connected to any service, but she can connect to WiFi, so she and I can use Facebook Messenger instead of texting. That's true for a lot of our clients, because phones get turned off and on all the time, numbers change all the time. I can still reach them on Facebook, on Facebook Messenger. You can log in to any computer or any phone to access it.

As we will discuss further in Section 4.3, participants' and their clients' threat models also influence their choice of communication method.

4.2 Threat Models and Security Concerns

We now turn specifically to the threat models and computer security related concerns voiced by our participants, both for themselves as individuals and representatives of their organizations, and on behalf of their clients. We found that many of the security concerns or goals that our participants voiced ultimately revolved around preventing revictimization and protecting the physical safety of clients and VSPs. In this work, we focus primarily on technology-related issues, but highlight other concerns as well where necessary for context.

4.2.1 Trafficker as Primary Adversary

The most common adversary for VSPs and clients were the clients' former trafficker(s) or potential future trafficker(s).

Compromising Online Accounts and Communications. VSP clients' communications may be compromised by traffickers, either digitally or via physical access. In many cases, traffickers have access to account credentials directly. P5, who works with labor trafficking survivors, described one tactic traffickers use to gain such access and alludes to the way low digital literacy can harm international and/or labor trafficking victims:

> P5: What if their trafficker has access to their email or helped them set up the email account. Just the client never knew that and now I'm communicating with the client and [the trafficker] is reading our information?...I feel with our clients, they're just so vulnerable and a lot of them were brainwashed...using a cell phone or using Facebook, a lot of them, their traffickers opened the account for them and they think, "Oh he was just being helpful. He wanted me to communicate with my family."

Traffickers may also compromise or intercept communications via physical access to clients' devices. For example, in the sex trafficking ecosystem:

> P7: I've had different guys that'll pick up [my clients'] phone and pretend to be them, go through their messages.

Despite the risk that a trafficker might physically see or digitally intercept communication intended for a victim, P1 weighed such risks against the benefits of reaching trafficking victims in her text outreach work. Note that the term "pimp" is another way of referring to the trafficker.

> P1: And I don't think it's at the expense of the victim, okay? I think, people ask this question because they're like, "Well don't you think that their pimp is gonna beat them up because they got this message?" Potentially. 100% yes...It's either, I get information out there that will potentially give them an out, or they just don't get anything.

Tracking Location. Another concern was traffickers tracking down former victims after their escape. P16 has had clients who found GPS trackers on their cars; P7 described the use of tracking apps on phones:

> P7: It's usually...through [the victims'] device because most of the pimps get [the device], so they have the family tracking, different apps and stuff like that...One of my girls has shown me that they can pull it up on their computer and you can see where all of [the victims] are at one time.

Using Online Information to Track Down Survivors. Even if a survivor's devices or accounts are not directly compromised, participants worried about the use of online public information to track down survivors. This fear is exacerbated by the fact that the trafficker often knows key information (like birth date, social security number, etc.) that allows access even to protected information.

For example, P14 is herself a survivor, and she generalized from her own experiences the ways traffickers can utilize public information to relocate survivors. Specifically, she explained that traffickers can find where survivors have moved by searching publicly available Department of Motor Vehicles (DMV) records; they can use survivors' addresses and social security numbers to access and potentially lock them out of their own bank accounts; and they can then track survivors' activities by observing the details of bank transactions.

As another example, P17 described being found via medical records and an old Facebook page she had thought was gone. P16 talked about how shared rewards systems (like grocery rewards cards) can reveal to a trafficker where a survivor is shopping and what they are purchasing.

Undermining VSP Operations. Participants also discussed the ways that traffickers seek to undermine the efforts of VSPs. P7 talked about traffickers hanging out near VSPs to recruit, and P16 talked about a trafficker sending a victim into a survivor program to recruit others directly. P2 mentioned that traffickers have called her organization's hotline looking for survivors.

For shelters where the location is confidential, participants described various ways in which this confidentiality could be compromised. A common concern, for example, was that people living in the shelter might accidentally reveal its location (or the location of shelter guests) to traffickers via pictures or other posts on social media. P14 felt that location confidentiality was a challenging, if not impossible, goal:

> P14: ...how confidential really is any kind of building? I mean, you're gonna see it on Google Maps eventually. Whether or not you see it this year or three years from now when they do their next picture, you're gonna see it. So it's not gonna be necessarily confidential for long.

On a related note, P14 talked about an organization she knows that did drone footage of their safe house as a cautionary tale to VSPs of how easily location confidentiality can be breached.

> P14: Which to me, anybody who is logical, you're doing drone footage of a supposed safe house. Well, any good hacker is gonna be able to pinpoint on a map exactly where that safe house is. Now, you're no longer safe.

4.2.2 Other Threats and Concerns

Beyond traffickers as direct adversaries, our interviews surfaced several other threats and concerns that VSPs and their clients may contend with.

Availability of VSP Resources. VSPs have limited resources which can come under intentional or unintentional contention. For example, several participants discussed ways in which the availability of the emergency hotline can be impacted, either by suspicious callers or by callers who misinterpret the function of the hotline. For example, P12 talked about how the hotline gets calls from people who need help with their subway cards because there are posters with the hotline number in the city's subway system.

Post-Trafficking Limbo. Several participants (P11, P13, P15) discussed how sex trafficking survivors can be at greater risk for abusive or unhealthy relationships:

> P13: They'll minimize the [domestic violence] because "at least he's not selling me"...They'll minimize the psychological violence that they're causing them or the emotional.

P13 gave an example of the potential consequences, describing a client who has an abusive, controlling boyfriend:

> P13: Like, within the last two months she's gotten like four new numbers, four new phones or five new phones. So I'm starting to think that this guy is breaking all her phones so that she doesn't have communication with anyone.

P13 described how this constantly changing communication environment severely limits the amount of help she can offer the client, e.g., prolonging the process of helping her find employment. Prior work [27] describes how domestic violence can serve as a "push factor" into sex trafficking. Our findings suggest that the push factor can also work in the opposite direction from sex trafficking to domestic violence. Computer security in the context of intimate partner violence has also been covered extensively in prior work [5, 10, 11, 21].

Labor trafficking survivors are especially desperate to get a job, and P5 described how they will sometimes even consider asking people in their community back home (who got them into labor trafficking in the first place) about jobs for undocumented individuals. Furthermore, the internet is not always a safe place to look for re-employment. In describing ways that technology facilitates trafficking, P8 talked about online frauds that can lead to labor trafficking:

> P8: We've had clients who respond to certain Craigslist ads for either a place to live or a job and then once they get into this suspect situation end up...getting trafficked.

Online Triggers. Several participants mentioned the risk of online triggers that may push a sex trafficking survivor towards revictimization. For example, survivors who are friends with individuals still in sex work (whether voluntarily or not) are constantly bombarded on social media with reminders of their past (e.g., a friend might post about the amount of money she made in a night):

> P2: We talk about "environmental triggers," and you can avoid an area of town as part of a safety plan around relapse prevention, but do you also have to delete your Snapchat and maybe your Instagram? And maybe get a new Facebook? If you're still "friends," on any social media platform, with anyone from that life, you're gonna be seeing triggers constantly.

In a similar vein, P4 worried about all the things her (underage) clients might stumble across on the Internet. She told the story of a time one of her clients was doing homework and clicked on a Youtube video. Youtube's content suggestions led the viewer to increasingly explicit content. P4 was also fearful that images of past (digitized) exploitation might surface on the Internet and haunt her clients later in life.

Concerns around Law Enforcement and Legal Systems. Both VSP staff members and survivor leaders voiced concerns related to the interactions between victims/survivors and law enforcement. On one extreme, a survivor leader explained that local law enforcement was complicit in her trafficking. This is a real concern — e.g., police officers in New York City were recently charged for involvement in a prostitution enterprise [31]. Thus, this survivor worried that, if law enforcement ever came to the shelter (to help with some emergency), this could be triggering for shelter residents who may have had negative experiences with law enforcement. Participants also voiced concern over victims of trafficking being charged with crimes. For example, prostitution is largely illegal in the United States, and sex trafficking survivors may be charged under prostitution laws or with other crimes committed during the time they were being trafficked [26, 27].

Participants also expressed frustration over regulations that make it difficult to establish trust with clients, such as legislation in some states requiring advocates to report runaways who come to their shelter to parents and law enforcement. This disincentivizes minors to come to the shelter:

> P10: If they're listed as missing or as a runaway, I'm obligated to let law enforcement know where they are...I do have a lot of professional protocols I have to follow as well. I adhere to those, as much as they suck. Our laws just don't always enable us to do what actually needs to be done.

As we discuss in Section 4.3, these concerns can drive the communication choices of clients and VSPs. We also want to note that some participants described strong partnerships with law enforcement, and one survivor leader described the immense support she received from law enforcement in her recovery.

Authenticity of First Contact. Finally, for VSPs who do direct outreach to potential clients, it is difficult to convince the recipient of their good intent. P1 reaches out to potential sex trafficking victims via text message, and those receiving her text messages are sometimes fearful that she is the police. P5 has heard about this kind of outreach, but has not started using it because she knows the individuals she would be reaching, potential labor trafficking victims, would be highly supicious:

> P5: It's like, "Should I trust this?"... "Should I respond to that or is it just another trap for me? Am I going to get in trouble?"

Victims' concern about both traffickers and potential legal ramifications, discussed above, may lead to this skepticism.

4.3 Technical Defenses and Mitigations

We now consider the concrete steps that VSPs take to mitigate their own and their clients' computer security and privacy related concerns (with the ultimate goals of avoiding revictimization and other harm, as discussed above). Overall, we observed four categories of technology-related defensive strategies: (1) guiding or explicitly restricting how clients use technology, (2) protecting communications with clients, (3) protecting data about clients, and (4) protecting the VSP's resources and employees. These strategies are in addition to physical and non-technological defenses, e.g., security cameras and bullet-proof windows in shelters, and heuristics that VSPs use to identify suspicious hotline callers.

4.3.1 Guiding Client Technology Use

In order to protect clients from revictimization or other threats, VSPs guide—or in some cases, explicitly restrict—their use of technology. This guidance is typically done in the form of safety planning with a client, or through rules and guidelines about the use of technology in a shelter.

Technology Safety Planning. VSPs work closely with their clients to help them be safe and feel safe. Given our focus on computer security, we focus primarily on technology safety planning here, but note that other forms of safety planning (e.g., for physical and emotional safety) are related.

One key goal of technology safety planning is to keep a client's whereabouts hidden from a former trafficker. Participants talked about a variety of strategies, including avoiding different parts of town, overhauling communication methods and social media accounts, and turning off location services on devices. For example:

> P10: Some people, they need to create a whole new social media everything, change their phone number and email address, and they need to just like literally disappear... That means that your accounts are completely, 100% locked down and you have pseudonyms, and you don't use your face in any pictures that you post. You never post your location. You don't have location turned on on your phone. You get a brand new phone because you don't know what kind of app trackers there are.

Some participants simply give guidance to clients, while others, like P10, actively help clients configure their devices:

> P10: I tell them . . . "Give me everything. Give me all the stuff." I sit down and lock everything down.

Our survivor leader participants described the precautions they take themselves and would recommend to other survivors. For example, P14 only uses location services when she needs help with navigation, changes her passwords regularly, and avoids making location-tagged posts on social media. Likewise, survivor leader P17 uses pseudonyms on her profiles and deactivates her Facebook regularly. In addition:

> P17: When I'm at the store and they're like, "Can we please have . . . your zip code or your phone number," I always say no, my phone number is very private. When I check in at hotels, I always have a process so my name doesn't associate with the hotel. My medical information is protected like everybody else's but I always have to have a conversation, like look, there are people that have every piece of information about me and they will call to get my medical information so I need a code word or something associated with my account.

While a common sentiment was that location services on phones should be turned off, on the flip side, clients sometimes want location services *on* as part of the safety plan:

> P2: We've had some clients...who want their location services on, so that I can use my iPhone and find them if something goes south, or to get an Uber sent to them in a crisis, or whatever the case may be. They want us to be able to track them.

Participants also helped their clients with general online safety best practices, For example, some participants (e.g., P11, P15) talked about helping their clients understand that folks on the Internet cannot always be trusted:

> P15 (who works with sex trafficking survivors):

> We've had some residents, when they're here, they start dating again. So they're on Facebook, they're on different websites, so I have candid conversations, "Okay, are you telling someone where you're gonna go? Are you telling another friend where you're meeting this new person online? What time can we expect you back?" Things like that. Trying to put that idea into their head that you should not trust people on the Internet.

Overall, there was the sense that safety planning is individualized rather than one-size-fits-all. For example, P14 mentioned that factors like how long someone was trafficked and where and whether or not the individual has made changes to personal appearance (e.g., dyeing hair) all impact safety planning. P15 also mentioned how age plays into technology use and, subsequently, technology safety planning: clients in their 40s and 50s tend to not have a large social media presence in the first place, while younger clients find it much more difficult to take a social media hiatus.

Stepping back, we observe a tension between granting autonomy to clients and providing maximum security:

> P15: Because I always bring up to people, you probably should turn off location on your phone. But I do kind of leave it up to them. It's not mandatory that they turn it off. 'Cause we come from an empowering place. We don't want to be telling them what to do.

In addition, working through potential threats and how to defend against them can be highly stress-inducing — one of the challenges mentioned by our participants revolved around balancing the client's safety with their mental health. P8 talked about being careful in safety planning to not trigger the client and cause the client to become more fearful. P14 talked about the fine balance between making someone untrackable and keeping them sane. P15 pointed out that the survivor most likely is already safety planning and is in the best position to look out for himself or herself.

Shelter Technology Rules. Participants described sometimes enforcing technology-related rules in shelters. A number of rules or guidelines centered around attempting to protect the identity of people in the shelter and the confidentiality of its physical location. For example, some shelters disallow photos or videos:

> P1: We have to think about all our clients and their privacy, especially we say, "If you're taking a photo, somebody could be walking behind you and you've breached their privacy because somebody could know who they are."

Similarly, P16's organization asks that shelter residents refrain from posting on social media and turn off location services on their devices. These rules aim to prevent accidental disclosure of the shelter location through, say, a Facebook post containing the resident's location. At P4's organization, these rules hold for visitors as well: P4 mentioned that visitors have posted photos of general surroundings and staff asked them to take them down. P16 said that they also put up a sign notifying clients that if they use the VSP main office WiFi they are vulnerable to being tracked to that location — but overall considered providing WiFi to clients more important than mitigating this risk by not providing WiFi.

Additionally, some participants mentioned restricting or monitoring how clients use the computers provided in shelters, with the goal of shielding clients from content or activities that might put them at risk of revictimization. For example, at P3's organization, advocates ensure that clients are not using computers to post sex ads. In addition, clients can set up email accounts for employment, and they are told outright that the accounts are not private (i.e., the advocate may inspect the client's emails if there is cause to believe that the client is using the email account for other purposes).

In general, we found that organizations who work with younger clients (under 18) have more regulations around technology usage. For example, P4 checks the browsing history of the shelter's computers weekly. P6 was in the process of purchasing software to help manage computer usage. Her organization has an adult sit with clients who need to use a computer. At the under-18 shelter run by P9's organization, clients physically check in their phones when they enter.

The main challenge here lies in balancing technology rules with the fact that technology use is an increasingly crucial part of life for many people, helping them feel "normal." And, as P14 explains, strict restrictions on technology use can actually undermine security goals:

> P14: If we deprive them of that technology, they're gonna do it behind our back. They're gonna find a way to get a burner phone, they're gonna find a way, and a friend, and whatever to get a phone ... whether we endorse it and give them a safe way to do it, or whether we let them do it behind our backs and potentially risk all of us ...

4.3.2 Protecting Communications with Clients

Given the potential for compromise—by traffickers or others—of communications with clients, VSPs carefully consider their choice and use of communication methods.

Choice of Communication Medium. Participants discussed two main goals when selecting communication methods: (1) protecting the content of communications from potential adversaries and (2) maintaining contact with clients. We summarize the pros and cons of communication methods from the perspectives of advocates and clients, with respect to both convenience and security, as reported by participants.

SMS. Participants described SMS, or texting, as common and useful. It gives survivors space to choose whether to respond to VSPs or not, allows for urgent communication and quick

access to resources, and is more discreet than phone calls.

P7 suggested that individuals in the sex trade (whether voluntarily or not) are moving away from using text due to concerns about law enforcement confiscating phones and searching text messages. From the advocate perspective, some participants expressed unease that, with texting, there is no authentication ensuring that you are communicating with the person you think you are communicating with.

Phone. Talking on the phone, by contrast, allows participants to authenticate communication partners via voice:

> P15: Texting can be tricky. Even if I've worked with the client for a while and I'm still texting them. Sometimes it's like I'd rather just call and talk to them so that I know it's them talking to me and not someone else on their phone.

Phone calls were also generally considered a sufficiently secure communication method—as long as the line is not being tapped. However, clients were sometimes not comfortable talking on the phone when they were still in physically dangerous situations.

Social Media. Social media — especially Facebook — emerged as a very popular way for VSPs to communicate with clients. (Indeed, related work on technology in the trafficking ecosystem [2] has found that victims of domestic minor sex trafficking utilize Facebook in app and website form more frequently than any other online service.) We observe that this prevalence may cause challenges, as social media can blur the personal/professional boundary between VSPs and clients, and it may not be secure: our own findings as well as prior work on intimate partner violence [10, 11] suggest that abusers commonly access victims' Facebook accounts.

In our interviews, however, the benefits of using social media to communicate with clients seemed to outweigh these risks. A key benefit of Facebook was that clients could retain access to it when they switch devices or phone numbers, and that using it does not require a cell phone plan:

> P7: Facebook. All the time. 'Cause they can always go to the library and get on it. They can always go somewhere and get on their Facebook.

Some clients consider Facebook to be a more discreet communication method compared to phone calls:

> P7: And more of them use Facebook because they don't want somebody calling their phone or having access to their phone. I've had a couple people that are like, "Do not call this number ever. I will call you. Don't ever leave a message on this number, don't ever call it, don't ever do anything, 'cause I have this one chance to call you and if you call back, it's going to be bad for me."

Snapchat can play a similar role, with the additional benefit of supporting disappearing messages by default. P6 recounted the case of a client who ran away from foster care but remained in touch with — and eventually asked to be rescued by — someone at P6's organization via Snapchat. Here, the client's use of Snapchat may have helped protect the communication from being discovered by the trafficker.

Email. By contrast, email was not mentioned as a common or convenient communication method, largely because of a lack of access by clients. For example:

> P12: ...a lot of them don't have e-mail. If they do, they don't know how to access their e-mail. Somebody else helped them set up their e-mail and they forgot the password and their username...

Though (according to P4) email can be helpful as a last-ditch attempt to establish communication when a client's phone number has changed, participants generally described preferring Facebook Messenger in this situation.

Secure Communication. Despite the serious security and privacy concerns faced by our participants and their clients, we heard very few cases of VSPs using existing secure communication technologies with their clients. P16 was an exception:

> P16: ...we like WhatsApp because it's encrypted and because it's a safe storage for the conversations. We cannot use Facebook or Instagram or Snapchat because it's not secure. I know a bunch of programs that will respond through Facebook Messenger and we're not going to do that especially with all the privacy concerns.

We hypothesize that the limited use of WhatsApp (and no mention of other secure communication tools, such as Signal) reflects the tendency of VSPs to choose communication methods that are already familiar to clients (e.g., Facebook or Snapchat in some cases, or texting and phone calls in the cases where professional boundaries preclude social media use).

In Person. Participants also used a non-technological strategy for mitigating digital security concerns: meeting their clients in person. Meeting in person has the benefits of avoiding communicating through any potentially compromised digital medium and allowing for the authentication of the client to the VSP (and vice versa). For example:

> P15: I think in terms of texting with clients and what not, I really prefer to meet someone in person. Especially if I'm meeting someone new. If my first contact with someone is through text message, I don't know if it's that person talking to me. I don't know, it could be their trafficker, could be someone lying to me, making up a name to try to figure out where the house is.

We note that meeting in person cannot defend against the case where a client's phone has been compromised by an adversary who uses it as a remote microphone to eavesdrop on conversations. One participant took steps to mitigate this

risk: P8 obtained Faraday bags for the organization to use when there is concern that a client's device might be compromised (it blocks incoming and outgoing signals from the device). P8 talked about using it with a client and how it allowed them to talk more freely without fear of being monitored. The downside of meeting in person is that it can be challenging for survivors to get to the VSP. P16 stressed the importance of technology in this context:

> P16: They are working three jobs, the kids are home alone, they want to be home with the kids so I think that's actually a nice example of how technology is so helpful for us. They like physically, economically, emotionally cannot get to an appointment but...if we can communicate through a text that could be the lifeline. Or email.

Meeting a client in person also means that the VSP knows, by definition, where the client is physically located. This can be at odds with a VSP's desire to avoid turning a client in to law enforcement, e.g., as would be required if the client is listed as missing or as a runaway. P7 discussed how communicating digitally can provide a loophole for this case:

> P7: You can hit me up for services and tell me, "I need this, this, and that,"... But if I don't know your location, I can't report you... I don't know where you are. It kind of covers our back because we can still serve them without having the legality to report them.

Message Content and Authentication. No matter the chosen communication method, there is always the risk of the trafficker or another adversary monitoring communications in real-time or reading them later, e.g., by leveraging access to a client's account, or by simply overhearing a phone call. To mitigate such a threat, participants reported using ad-hoc techniques to obfuscate the content of their communications with clients. For example, P1 is very brief in her phone communications with clients and checks in beforehand to make sure it is a good time to talk. P10, P3, and P7 use predetermined codewords or code phrases when communicating with clients via SMS or social media. P7 described an authentication strategy in which her client asks or answers a specific question that they established previously to start off communication.

New Devices. P8 reported clients getting new devices as a safety precaution. Limited financial resources on the part of VSPs constrain how much VSPs can help clients acquire new devices. Typically the phones provided by VSPs come from sources such as government programs or Verizon's HopeLine program (which provided recycled phones to domestic violence survivors but is now phasing out). P16's organization receives donated phones but does not have funds to purchase data plans. They still give the phones to clients as a way to call 9-1-1 in the case of an emergency.

Challenges and Tensions in Protecting Communication. In addition to learning about existing ways participants work to protect client communications, we also explored their reactions to other technologies: single-use URLs and disappearing messages [1, 8, 9]. These explorations surfaced several challenges and tensions.

First, a risk with securing a communication channel is that it may make it more difficult for a client to access information. For example, several participants pointed out that although single-use URLs may prevent an adversary from accessing sensitive information via an already-used link, they also prevent the client from *re*-accessing that information.

Second, participants explained that appearing to hide something can put a client in danger (e.g., causing the trafficker/exploiter to become violent):

> P7: Any way that somebody can open the thing and tell that you're being secretive is a scary thing. 'Cause then you're hiding something from me. "What are you doing behind my back? Who are you telling?" There's a lot of paranoia...

The above quote came up in the context of disappearing messages that require a password to view the message, but we observe that this tension may arise for any communication tool that clearly has security as a goal. On a related note, participants described the strong psychological power traffickers have over their victims. P6 discussed how traditional security mechanisms (such as passwords) may fail as the trafficker has such power over the victim that he or she can easily compel the victim to reveal secrets.

> P6: Because they have been so conditioned, so coerced, that it's [the victims] telling anything that they're asked...They're the ones that have a problem keeping a secret.

4.3.3 Protecting Data About Clients

Participants talked about the strategies they use to secure the data that VSPs collect and store about clients.

Access Control for Internal Databases. Most participants talked about using databases to store client information. A few participants explicitly mentioned how each staff member at the organization has their own login credentials and also talked about access controls on the data.

> P15: Someone working in our admin department, like a secretary, they shouldn't be able to open our case notes. There's that kind of protection.

P15 was concerned about the cloud-based nature of the case notes software her organization uses. She was worried that if staff members logged in at home, client information could be seen by the staff member's family or roommates.

Interactions with External Organizations. P7 described how technology aids the referral process and how protocol

dictates that sometimes meetings must take place in person:

> P7: We have a secured email that people can send referrals to...so we get a lot of our referrals from social workers and different people like that. Or I'll have a teacher or a counselor be like, "I can't give you much information, but I'd like you to come in and meet with ..." 'Cause they can't send it over social media or emails, anything.

Several participants described strict protocols for sharing client information with external organizations:

> P15: We have a very specific release form. So if someone wants me to connect with their substance abuse worker that they're working with, I need that form filled out with that substance abuse worker's name, my name, the client's name, the client's signature saying you can tell this substance abuse worker ... You can tell them my name and my date of birth. We ask them to be very specific.

Securing Internal Communications. P15's organization uses encrypted email internally. Other participants mentioned strategies for protecting client identities in internal communications more informally, such as using client initials or first names only in communications and files:

> P8: We're also very careful about using client names. Even in inner work emails or text messages or anything like that. I have all my clients saved in my work phone just as initials. So even if someone is reading a text conversation, they wouldn't know who that was with. Within our database system, everyone is assigned a client number, so we do often use that when we're emailing.

Minimizing Data Collection. Finally, participants described a general principle of storing the least possible amount of client data:

> P16: We intentionally don't write...detailed notes and don't jot down information that could potentially harm them. Not even casually because even if we make a note on the intake form or we write down on a post-it that's technically a part of the case now. ...Keep it brief, keep it vague, keep it objective because anything can be used against the client in court.

In some cases, though, collecting sensitive data is necessary or useful. For example, P13 described how other staff members at her organization make copies of a client's important documents during intake (e.g., birth certificate, Medicaid card, ID, etc.). P13 does not do so, because she considers this information to be sensitive — but she pointed out that the copies can be critical when a client loses the original document.

4.3.4 Protecting VSP Resources and Employees

Finally, we turn to the strategies that VSPs use to protect their own resources and staff.

VSP Location Confidentiality. Participants described various strategies for keeping the location of the VSP's office or shelter confidential. In addition to the shelter technology rules described above, some participants described protecting the address of the shelter by not mentioning it in digital communications with clients. For example, P8 specified that the office address is never texted or emailed out. Likewise, P16 does not share the shelter address. Instead, clients are given the address of a neutral location several blocks away and staff meet them there and bring them to the shelter. Other non-technical strategies for protecting the VSP's location include requiring clients and visitors to sign a confidentiality form, asking clients arriving in a Lyft or Uber to be dropped off several blocks away, only meeting clients at the VSP office if absolutely necessary, and making the shelter look physically inconspicuous (e.g., like a vacant office building).

Personal/Professional Boundaries. Participants described attempting to separate their personal and professional lives, to protect their own physical and emotional well-being.

The primary technical strategies participants described involve separating personal and professional communications. Almost all participants mentioned having separate work emails and work cellphones. With respect to social media, some participants had a strict policy of not interacting with clients on social media (e.g., finding it unprofessional), while others found it invaluable for reaching and maintaining contact with clients (as discussed above).

Participants who do use social media to interact with clients often use separate personal and professional social media accounts. For example, P7 talked about how her personal Facebook account has strict privacy settings, and how she made her friends list inaccessible on her work account to protect those friends. P2, who generally works with individuals who (voluntarily or not) are in the sex trade, talked about carefully regulating when she looks at her work Facebook account because she does not know what she might be exposed to. Another possible concern is that Facebook may unexpectedly reveal to traffickers or others the connection between survivors and VSP staff members (e.g., by suggesting a VSP staff member as a friend to a trafficker through the "People You May Know" feature [15]), but this concern was not mentioned by our participants.

Participants also mentioned a variety of non-technical strategies for protecting themselves, including meeting clients in public locations, letting others know where the participant is going to meet a client, being vigilant of physical surroundings, and the importance of personal self-care and therapy. Ultimately, however, participants accepted the inherent risk in the work that they do:

> P6: I don't make any claims that we're gonna protect [volunteers] from something bad happening. But then, it happens with these girls all the time. And if we're not willing to walk into that garbage in danger with them, to me it's kind of the same as throwing them out to the wolves. 'Cause they can't get out. They can't choose to not be at risk.

5 Discussion

We now take a step back from our findings, surfacing broader lessons and making concrete recommendations for technologists wishing to support VSP-client interactions.

5.1 Broader Lessons for Technologists

Tensions and Challenges. Our findings surface a number of tensions and challenges that influence how VSPs and their clients use technology. These must be understood and considered by technologists wishing to work in this space.

Limited resources on the part of both clients and VSPs. For example, clients may not have access to cell phone plans, limiting their communication technology choices to those that support WiFi (e.g., Facebook Messenger). They also may have limited memory on their devices, or may frequently change devices and phone numbers. Technology solutions must take into account these potential limitations.

Limited and varied technology expertise. We found that computer security and privacy literacy and practices varied widely among VSP staff and clients. Participants' defensive strategies ranged from technologically advanced (e.g., using Faraday bags) to abstaining from technology. Participants described knowledge gaps among clients (e.g., clients not realizing that their Facebook profiles can be found via a web search), but we also spoke with survivors who are going to extensive lengths to protect themselves digitally. Technology must be designed for this range of knowledge and expertise, and there may be a role for computer security education and training specifically designed for VSPs and their clients.

Balancing client trust and technology access with safety. VSPs must balance building client trust with enforcing rules intended to protect clients and the VSP. As one of our participants put it, a VSP that it is too strict in terms of rule enforcement risks becoming, in some ways, like a trafficker to its clients. Even well-intentioned rules and guidelines around technology use can ultimately reduce safety as clients figure out ways to circumvent the rules. Thus, our participants commonly gave clients space to make their own technology-related choices (echoing prior findings about journalists deferring to the choices of their sources [22]).

Double-edged sword of technology. Access to technology can be a critical part of recovery — survivors can connect with new or former support networks, communicate with VSPs, and use technology for job searches and other critical tasks. However, this same access opens survivors up to potential risks, including being tracked down or monitored by former/future traffickers and being exposed to content that may make recovery harder. This tension echoes findings in the domestic violence context [21].

Balancing safety planning with client mental health. Finally, solutions must take into account the trauma and psychological challenges that survivors face — and avoid "triggering" survivors or causing them to be unnecessarily fearful.

Lack of Systematization and Need for Personalization. Our findings suggest that there is little systematization among VSPs around technology in VSP-client interactions and safety planning. For example, one organization uses WhatsApp because they perceive it to be more secure than Facebook, while many other participants discussed commonly using Facebook to communicate with clients. These differences may stem from factors such as: differences in the technology expertise and experiences of the VSPs and their clients; the fact that, in some organizations, VSP staff work relatively independently without top-down restrictions; and the fact that different clients face different risks and thus different mitigation strategies are necessary or effective.

These observations lead us to two conclusions: First, there may be benefit in systematizing computer security related guidelines and trainings for VSP staff, to help inform them about potential risks and benefits with different technology choices. Second, technology-based interventions cannot be "one size fits all" but must enable personalized approaches for survivors and VSPs in different situations.

5.2 Directions for Technologists

Authentication and First Contact. Technology can help VSPs reach out to potential clients, e.g., through the text messaging program discussed by some of our participants. However, a challenge with directly contacting trafficking victims or survivors is how to authenticate the first contact and build trust. There may be opportunities for technology designers to help address this challenge, e.g., through the (re)design of messaging tools for this population or through rigorous A/B testing of different message content for direct outreach to potential clients.

In the other direction, some participants discussed how difficult it can be for clients to find or contact VSPs when they are looking for help. Possible technology-based improvements here include real-time chat systems to replace phone hotlines (as "sometimes picking up the phone...is not an option", P7) and proactive help by search engines that suspect a user is attempting to find trafficking-related resources.

Designing for VSP-Client Communications. Based on our

findings, we recommend those designing for secure (i.e., hidden from the trafficker) client-VSP communications take into account the following lessons:

- Raising the trafficker's suspicions can be dangerous, so sensitive messages should look innocuous or be easily hidden to provide plausible deniability around the content, intent, and/or recipient of the message.
- It is also important to account for the complex psychology of the victim-trafficker relationship, and how this makes it challenging for the victim to keep secrets (e.g., passwords) from the trafficker.
- Solutions must work with devices with varying levels of functionality (e.g., phones with limited memory) and in the face of changing phone numbers and devices.
- It is important to plan for adversaries (traffickers) with physical access to a client's device.
- Solutions that can fit into existing popular communication platforms and/or existing VSP-client communication habits will have the greatest success in adoption.
- Prior work on domestic violence has shown that taking steps to remove an abuser's access to an account can be dangerous [11]. We suggest research on ways to support secure communication *within* otherwise compromised accounts, e.g., via a hidden secondary messaging interface.
- Finally, the client's ability to easily access and re-access the intended information is crucial — but must be balanced with protecting the same information from a potential local or remote adversary.

Publicly Available Information. The survivor leaders we spoke with are already extremely cautious in terms of digital security, yet there are data sources and tools/services that they have no control over that can compromise their safety. For example, traffickers utilize public records (e.g., DMV records) to track down former victims. To try to combat this, government address-confidentiality programs [23] provide qualified individuals with an alias mailing address. However, this is not a panacea; there are an unknown number of third-party services that pull public data and market themselves as an easy way to find people on the Internet. Even if a survivor qualifies for the confidentiality program, sensitive data could already exist on these people-finding services, and it is unclear how long it takes for new information to replace old.

Furthermore, this problem affects the general public as it enables a host of other crimes such as stalking and "doxxing" (releasing sensitive information publicly). We suggest future work study this ecosystem and develop solutions for helping people protect themselves — for example, streamlining the process of opting out of these people-finding services and helping users renew the opt-outs when/if they expire.

Supporting Safe Technology Use in Shelters. We believe that the computer security and privacy community can work with VSPs to develop ways for shelter residents to safely utilize technology. This is especially imperative for VSPs working with youth. These VSPs are in a difficult position as the youth they work with tend to be avid technology users but may not understand all the risks inherent in active technology use. In addition, they may be using technology to communicate with unsafe individuals such as their trafficker or potential trafficker. We found that, in response, VSPs tend to take an approach of strict regulation of technology use for young clients in particular, locking up phones at night and heavily regulating and monitoring computer use. While this is done out of the best intentions to protect the clients, it is (as discussed) commonly circumvented by clients.

Thus, it is clear that technology abstinence is not a reasonable solution for client safety planning. These findings highlight the need for members of the computer security and privacy community to work with VSPs to develop solutions and/or provide education to help strike the right balance.

Integrate VSPs and Survivors in Solution Development. Finally, echoing an increasingly common refrain in usable security, we note that it is critical to design technologies in a way that is deeply informed by the needs, constraints, and use cases of target populations. Though our work provides a foundation for technologists working in this space, future researchers should continue to connect with VSPs and survivors to design and evaluate any technology interventions.

> P14: Getting advice from the people who are using the technology that y'all are creating is a big part of moving forward. Because the moment y'all stop listening...to those of us who us are on these front lines using this technology to help ... the moment that that stops happening is the moment that y'all stop growing and being effective.

5.3 Limitations

Our study is qualitative, not quantitative; thus, our sample size is small and does not allow us to draw quantitative, generalizable conclusions. Self-reported data also has limitations such as recall and observer bias. Additionally, our participants are based primarily in urban areas in the U.S. and our results relate mainly to sex trafficking and female survivors. Thus, our results do not represent all possible VSP-client interactions. We believe there is more to uncover with regards to providing services to survivors of labor trafficking and survivors of other genders. For example, P15 talked about how her organization opened a shelter for all genders, allowing them to take in labor trafficking survivors and families. These are areas that call for further exploration with regards to how technology plays into these new dynamics.

6 Conclusion

Victim service providers play a critical role in the recovery of survivors of human trafficking. In this work, we conducted 17 semi-structured interviews with VSP staff members and survivor leaders, surfacing the ways technology is involved in VSP-client interactions, as well as the computer security and privacy concerns and mitigation strategies associated with those interactions. Key contributions of this work include detailing the various tensions that VSPs face when using technology in their interactions with clients and providing concrete recommendations for technologists who wish to support VSPs and trafficking survivors.

7 Acknowledgements

We are deeply grateful to our participants for taking the time to share their experiences and perspectives. We thank Kirsten Foot and Tadayoshi Kohno from the University of Washington for their invaluable help and advice throughout this project. We thank Robert Beiser, Sherrie Caltagirone, Kelly Mangiaracina, Lauren Moussa, Taylor Naber, Johnna White and other members of the anti-trafficking community for their assistance in developing the interview protocol and facilitating connections within the VSP community. Tiffany Chen and Kiron Lebeck kindly read the draft of the paper. Finally, we thank the anonymous reviewers for their feedback. This work is supported in part by the National Science Foundation under Awards CNS-1463968 and IIS-1748903.

References

[1] Disappearing Message. `https://onetimesecret.com/`.

[2] Vanessa Bouché and Thorn. Survivor Insights: The Role of Technology in Domestic Minor Sex Trafficking. Thorn, 2018. `https://www.wearethorn.org/survivor-insights/`.

[3] Virginia Braun and Victoria Clarke. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.

[4] Caliber. Evaluation of Comprehensive Services for Victims of Human Trafficking: Key Findings and Lessons Learned, 2007. `https://www.ncjrs.gov/pdffiles1/nij/grants/218777.pdf`.

[5] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. The Spyware Used in Intimate Partner Violence. In *IEEE Symposium on Security and Privacy*, 2018.

[6] DARPA. Memex (Domain-Specific Search). `https://opencatalog.darpa.mil/MEMEX.html`.

[7] Nicola Dell, Vidya Vaidyanathan, Indrani Medhi, Edward Cutrell, and William Thies. "Yours is Better!": Participant Response Bias in HCI. In *ACM CHI Conference on Human Factors in Computing Systems*, 2012.

[8] Martin Emms, Budi Arief, and Aad van Moorsel. Single Use URL Access Codes. `http://research.cs.ncl.ac.uk/cybercrime/no-follow-url.php`.

[9] Martin Emms, Budi Arief, and Aad van Moorsel. Electronic footprints in the sand: Technologies for assisting domestic violence survivors. In *Annual Privacy Forum*, pages 203–214. Springer, 2012.

[10] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. A Stalker's Paradise: How Intimate Partner Abusers Exploit Technology. In *ACM CHI Conference on Human Factors in Computing Systems*, 2018.

[11] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW):46, 2017.

[12] Felicity Gerry, Julia Muraszkiewicz, and Niovi Vavoula. The role of technology in the fight against human trafficking: Reflections on privacy and data protection concerns. *Computer Law & Security Review*, 32(2):205–217, 2016.

[13] Catherine Glenn and Lisa Goodman. Living with and within the rules of domestic violence shelters: A qualitative exploration of residents experiences. *Violence against women*, 21(12):1481–1506, 2015.

[14] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H Mhaidli, Kentaro Toyama, and Florian Schaub. Keeping a Low Profile?: Technology, Risk and Privacy among Undocumented Immigrants. In *ACM CHI Conference on Human Factors in Computing Systems*, 2018.

[15] Kashmir Hill. How Facebook Figures Out Everyone You've Ever Met, November 2017. `https://gizmodo.com/how-facebook-figures-out-everyone-youve-ever-met-1819822691`.

[16] ILO and Walk Free Foundation and IOM. Global Estimates of Modern Slavery, 2017. `https://www.ilo.org/global/topics/forced-labour/statistics/lang--en/index.htm`.

[17] Mark Latonero, Genet Berhane, Ashley Hernandez, Tala Mohebi, and Lauren Movius. *Human trafficking online: The role of social networking sites and online classifieds*. University of Southern California, Center on Communication Leadership & Policy, 2011.

[18] Mark Latonero, Jennifer Musto, Zhaleh Boyd, Ev Boyle, Amber Bissel, Kari Gibson, and Joanne Kim. *The rise of mobile and the diffusion of technology-facilitated trafficking*. University of Southern California, Center on Communication Leadership & Policy, 2012.

[19] Mark Latonero, B Wex, M Dank, and S Poucki. *Technology and labor trafficking in a network society*. University of Southern California, Center on Communication Leadership & Policy, 2015.

[20] Nelson Lim, Sarah Michal Greathouse, and Douglas Yeung. The 2014 Technology Summit for Victim Service Providers. RAND Corporation, 2014. https://www.rand.org/pubs/conf_proceedings/CF326.html.

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

[22] Susan E McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. Investigating the Computer Security Practices and Needs of Journalists. In *USENIX Security Symposium*, 2015.

[23] National Network to End Domestic Violence (NNEDV). Address Confidentiality Programs. https://nnedv.org/mdocs-posts/state-by-state-listing-of-address-confidentiality-programs-2016/.

[24] Polaris. On-Ramps, Intersections, and Exit Routes: A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking. Polaris, 2018. https://polarisproject.org/a-roadmap-for-systems-and-industries-to-prevent-and-disrupt-human-trafficking.

[25] Rebecca S Portnoff, Danny Yuxing Huang, Periwinkle Doerfler, Sadia Afroz, and Damon McCoy. Backpage and Bitcoin: Uncovering human traffickers. In *23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2017.

[26] Samantha Raphelson. Cyntoia Brown Case Highlights How Child Sex Trafficking Victims Are Prosecuted, December 2017. https://www.npr.org/2017/12/01/567789605/cyntoia-brown-case-highlights-how-child-sex-trafficking-victims-are-prosecuted.

[27] Dominique E Roe-Sepowitz, Kristine E Hickle, Jaime Dahlstedt, and James Gallagher. Victim or whore: The similarities and differences between victim's experiences of domestic violence and sex trafficking. *Journal of Human Behavior in the Social Environment*, 24(8):883–898, 2014.

[28] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. Computer Security and Privacy for Refugees in the United States. In *IEEE Symposium on Security and Privacy*, 2018.

[29] Jennifer Stoll, W. Keith Edwards, and Kirsten A. Foot. Between Us and Them: Building Connectedness Within Civic Networks. In *ACM Conference on Computer Supported Cooperative Work (CSCW)*, 2012.

[30] United Nations Office on Drugs and Crime (UNODC). What is Human Trafficking? https://www.unodc.org/unodc/en/human-trafficking/what-is-human-trafficking.html.

[31] Michael Wilson, Nate Schweber, and Ashley Southall. Brothels, Gambling and an Ex-Detective Mastermind: Officials Detail N.Y. Police Scandal, September 2018. https://www.nytimes.com/2018/09/13/nyregion/nypd-officers-arrested-prostitution-gambling.html.

[32] youth.gov. Transition & Aging Out. https://youth.gov/youth-topics/transition-age-youth.

A Interview Protocol

Our study involved qualitative semi-structured interviews. As such, the questions below served as a guide for our interviews, but individual interviews varied based on participants' responses and specific experiences. We let the participant's responses direct the conversation, asking relevant follow-up questions and skipping irrelevant questions as appropriate.

General Background

1. What is your job title and role? In your job, what are the main services you provide to clients?
2. Would you describe your technology comfort level as high, medium, or low? Why?
3. How many years old is your organization? How many employees are there? What are the main services your organization provides?
4. How do you refer to the individuals you work with (e.g., clients, survivors, participants, guests, etc.)?
5. What kinds of clients do you mainly work with? What type of exploitation have they endured? What is their nationality, their age range?
6. What are the most common pathways you see for your clients to be exploited? How has the rise of technology made the situation worse or better? What are your fears and hopes looking ahead?
7. FOSTA (Allow States and Victims to Fight Online Sex Trafficking Act) just recently passed. It amends section 230 of the Communications Decency Act so that laws relating to sexual exploitation of children or sex trafficking can apply to third-party content providers. How do you think the legislation might affect your work, if at all? How do you think it might affect the broader trafficking ecosystem, if at all?
8. What are the key factors that cause revictimization? How do you think technology facilitates revictimization, if at all? If you are worried a client has been revictimized, how (if at all) do you stay in contact with them?
9. How do you get help when you encounter issues with technology and computer security at work?

Client First Contact

1. How do cases typically come to your attention (e.g., law enforcement, community members, homeless shelters, victims directly reaching out, direct outreach, etc.)?
2. What means do you have for victims to directly contact your organization (e.g., phone, email, text, web form, online chat, etc.)?
3. Do clients ever reach out on their own? If so, how do you think they find you (e.g., word of mouth, Google, etc.)? What evidence do you have of this?
4. Walk me through what happens when an individual reaches out to your organization through any of those means. What do you do or not do to protect the individual's identity? How do you vet potential clients?
5. Is there an instance of someone contacting your organization that sticks out to you as particularly memorable?
6. Sometimes victims of trafficking are forced to recruit new victims. With that in mind, does your organization do anything to reach the traffickers, as some of them may be victims themselves?

Client Intake

1. How do you record and store client information? What do you or your organization consider confidential? What worries you most in terms of the security and privacy or confidentiality of the information? Are you worried that the information may be subpoenaed?
2. What do clients usually have with them when they arrive (e.g., devices)? Are there any rules regarding what clients are or are not allowed to have with them before receiving services and/or entering the shelter?

Day-to-Day Interactions

1. In your day to day work as you're interacting with clients, what are common (technology and non-technology) frustrations, worries, or fears? What would you say are the common frustrations, worries, or fears of your clients?
2. How do you communicate with clients in general (e.g., phone, email, SMS, social media, etc.)? For each mode of commuication:
    - How did you choose this mode?
    - What do you commonly communicate about?
    - Have you ever been afraid that someone might be eavesdropping on the conversation?
    - Are there things you purposefully avoid talking about or don't feel comfortable talking about via this mode of communication?
3. What access to technology do survivors have through your organization? Do you provide any devices, apps, software, web programs, wifi access? If there is a computer for clients: What do people use it for?

Additional Organization and Client Safety

1. Is the location of your organization and/or shelter confidential?
2. Do you have rules or guidelines about technology that clients have to follow (e.g., turning off location services on their phones)? Do you have rules or guidelines for visitors? How, if at all, do you enforce these rules?
3. What steps do you take to keep yourself safe? What are things you've noticed your clients doing to keep themselves safe?

Reactions to Prototypes

When presenting these prototypes, in order to minimize participants response bias [7], we explicitly told participants that we had not created the prototypes, that we were interested in both positive and negatives reactions, and that our goal in presenting them was to make the conversation around potential technology solutions more concrete.

We presented to participants two prototypes: single-use URLs and disappearing messages [1, 8, 9]. For each prototype, we asked participants:

1. Would you or your organization ever use something like this? What potential benefits, if any, do you see?
2. What would you change about this tool? Are there any new threats or concerns that it would raise for your clients or your organization?

Closing

1. If you had a magic wand and could solve any issue in this space, what would you do first?
2. What do you want to tell the computer security and privacy community to focus on with regards to helping victim service providers?
3. What drew you to participate in this study?
4. Is there anything you'd like to add about technology use in your job that I didn't ask about?