Navigating Security and Privacy Threats in Homeless Service Provision

Yuxi Wu[†][*], Ruoxi Zhang[◇][*], Shiyue Liu[◇], Mufei He[◇], Aidan Hong[◇],
Jeremy J. Northup[¶], Calla Kainaroi[§], Fei Fang[◇], Hong Shen[◇]

[†]*Northeastern University,* [◇]*Carngie Mellon University,*
[¶]*Point Park University,* [§]*Bridge to the Mountains*

Abstract

People experiencing homelessness interact with service providers to access essential services. As clients, homeless individuals are expected to reveal sensitive information about themselves to service providers, while personal security and privacy (S&P) preferences fall by the wayside. Simultaneously, providers take on S&P-adjacent responsibilities: helping clients fill out applications, safekeeping clients' personal documents, monitoring clients' online safety, undergoing workplace S&P training, etc. We created five storyboards to represent S&P challenges that clients can face when they interact with providers. In interviews with homeless individuals and service providers in the Northeastern United States, we use these storyboards to explore the S&P challenges in client-provider relationships within homeless services. We find a set of mismatches in S&P priorities between clients and providers, leading to mistrust between the two parties. We provide design recommendations, envisioned by both parties, for providers to bridge these mismatches.

1 Introduction

The homelessness crisis in the United States has grown significantly in the past decades [5, 50]. On a single night in 2023, roughly 653,100 people—or about 20 of every 10,000 people in the United States—were experiencing homelessness; this point-in-time count was the highest since reporting began in 2007 by the U.S. Department of Housing and Urban Development [43]. Between 2022 and 2023 alone, the number of people experiencing homelessness—which we consider as the lack of *"a fixed, regular, and adequate nighttime residence"* [42]—increased by 12% [43].

People experiencing homelessness interact with service providers to access essential services. As clients, homeless individuals are often expected to reveal sensitive information about themselves to service providers, even though security and privacy (S&P) may not be top of mind for them [52]. Even when they are unsure about giving up such information, they may feel compelled to do so anyway so that they can access shelter, health care, and financial support [15]. At the same time, beyond client intake, service providers may take on various S&P-adjacent and data management responsibilities [30], including helping clients fill out forms for other providers, safekeeping sensitive documents, monitoring clients' online safety, and undergoing workplace S&P training. While these actions may be invisible to clients, they can all contribute to how providers think about the S&P of their clients.

Previous research has identified a number of S&P challenges faced by homeless individuals, emphasizing financial insecurity, limited technology access, and untrusted relationships [23, 41, 52]. However, little focus has been given to how these challenges manifest when seeking essential public services. On the other hand, work in human-computer interaction (HCI) has offered important insights into the critical role service providers play in helping homeless individuals access these services, including how service providers' data collection practices can erode trust [4], and how formal support systems should be developed [20]. Our work contributes to these past lines of research by exploring both client and provider perspectives on these challenges, offering actionable insights for service providers to better support their clients.

Developing a better understanding of how S&P challenges manifest in client-provider interactions in homeless services will help the HCI and S&P communities develop more targeted solutions to support this marginalized population effectively. Therefore, we ask the following research questions:

RQ1 What S&P threats and concerns do homeless individuals face when interacting with service providers?

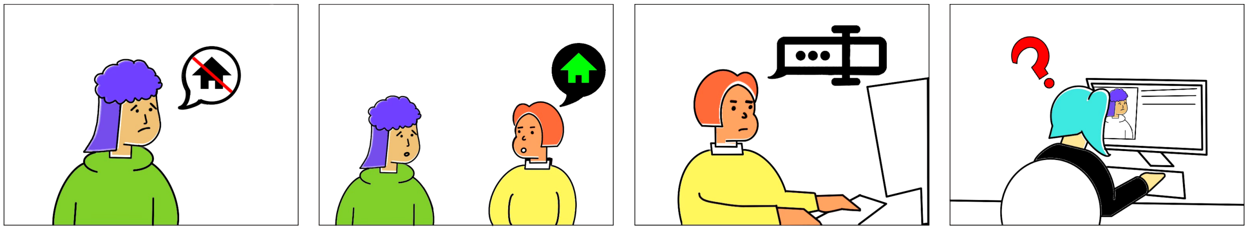
RQ2 How do service providers consider or address the S&P threats and concerns of their clients?

RQ3 What design opportunities do clients and providers envision for aligning their perspectives on S&P?

To answer these questions, we developed a set of storyboards and conducted semi-structured interviews and focus

---

[*] Yuxi Wu and Ruoxi Zhang contributed equally to this work.



Jordan has been homeless for three months and seeks help for affordable housing.

In a drop-in center, a service provider assists Jordan in applying for housing, collecting sensitive information.

The service provider fills the application on a shared computer in the office.They forget to log out.

Someone else in the office accesses the computer, finding Jordan's private information at risk.

Figure 1: We developed five storyboards of potential S&P challenges that people experiencing homelessness may come across when interacting with service providers. One storyboard shown above depicts Jordan, a homeless individual seeking support for their housing search at a drop-in center.

groups with both homeless individuals and service providers. S&P issues can be complicated and difficult for users to give feedback on, and our participants also faced challenges specific to their community (e.g., literacy, technical education, technology access). Following recent research [26, 54], we developed a series of five storyboards related to common S&P issues that might arise when clients interact with providers to access "lifelines" [13], e.g., employment, housing, health care, education, and social connection. These storyboards scaffolded our study sessions and provided participants with launchpads to discuss their own experiences.

We ran semi-structured interviews and focus groups with 12 people with experiences of homelessness and 8 service providers. We found evidence of a set of mismatches in S&P priorities between the two parties. Homeless participants mistrusted providers to keep their sensitive personal information safe; they also worried that asking questions about data use practices would get them dismissed as problematic or combative. Yet, provider participants shared experiences of extensive S&P-related training and vetting from their employers, and felt that they had created welcoming spaces for clients to receive S&P advice and support.

Our participants also suggested ways to put clients and providers on the same page regarding S&P. Homeless participants emphasized the need for stronger signals of trustworthiness from service providers, such as clearly-displayed certifications that providers had received appropriate S&P training. They also wanted more granular access control and consent-granting procedures for their personal files being shared within a service organization. Provider participants also revealed opportunities for formalizing ad hoc S&P behaviors. Several referred to the actions they took as "common sense" or as something they picked up on the job; hard-coding these into organizational protocols could help demonstrate further to homeless individuals that providers are taking their S&P seriously. Our study sessions themselves also helped raise awareness of S&P issues, as participants did not initially realize that some of their experiences "counted" as S&P.

In short, we uncover actionable ways for service providers to engender greater trust in homeless individuals when navigating S&P challenges. Through our storyboards, we explore the differences in how homeless individuals and service providers consider and perceive S&P in their interactions. These differences are manifested in the logistics of the interactions, the consent and agency of homeless individuals, individual S&P behavior, and organizational influences on S&P. We also find various design opportunities and recommendations for service providers to bridge those differences, such as bringing up S&P as a point of conversation in interactions, creating clearer signals of trustworthiness from providers, and promoting client self-advocacy and independence.

2 Related Work

Our work extends a rich body of literature on the influence of marginalization and life disruptions on people's technology use. Recent work in the area has tended to characterize "marginalized", "vulnerable", and "at-risk" communities as a broad population that requires certain design considerations [3, 10, 31, 34–36, 49, 58]. While people experiencing homelessness can be included in such populations, the intersection of homelessness with other vulnerabilities—gender identity, sexual orientation, race, health, intimate partner violence (IPV), etc.—can exacerbate the risks of such vulnerabilities and breed unique design and research challenges.

People experiencing homelessness, like any other population, use technology in their everyday lives [2]. They use mobile devices to maintain family and social relationships, including managing their self-presentation [27–29]. They access social media [19, 60], document and share their lives [59], and connect with others who are also experiencing homelessness [46]. However, a lack of reliable access to technology and digital resources may be especially disempowering to homeless individuals, who often need to use digital services to receive housing, health care [38, 39], financial support, etc. [32]. The more pressing nature of such "lifeline" necessities, can mean that S&P often falls by the wayside for people experiencing homelessness and financial insecurity [33], and the sense that "there's not much to take" can lead people experiencing poverty or with lower socioeconomic status to feel like their S&P is not worth protecting anyway [25, 48].

Simultaneously, there has been a relative dearth of literature directly tackling the S&P of people experiencing *homelessness* specifically, as a community distinctly different from broader financial insecurity and marginalization. In a recent survey of privacy research with marginalized groups, Sannon and Forte [49] examined only two works, out of 88 total, that specifically explored both homelessness and S&P. We thus limit our work's focus to two areas: the impact of homelessness on S&P, and the role social service providers play in protecting—or exposing—the S&P of homeless clients.

2.1 Homelessness and Security & Privacy

People experiencing homelessness face circumstances that make it uniquely difficult to prioritize S&P in their daily lives, instead deeming it a luxury [33, 48]. Sleeper et al. term these circumstances "tough times" [52]. We examine S&P work on financial insecurity, unemployment, and intimate partner violence to enrich our understanding of the tough times.

One such tough times challenge, *limited financial resources*, can put them at risk of being scammed and make it hard for them to opt out of giving up personal information. People experiencing homelessness need to submit personal information to apply for housing and jobs and access social safety net benefits; they may also submit information to enroll in loyalty card discount programs, at the cost of spam and unwanted ads. As another example, people might feel compelled to give up sensitive personal information to mobile loan apps for fear of being rejected for loans [41]. And, as Holten Møller et al. [23] found in a design fiction exploration, when people are unemployed and looking for work, they do not feel like they have agency over how their personal data is being shared and used. Finally, S&P violations themselves (e.g., phishing, identity theft, or having money stolen from a bank account) are exacerbated by limited financial resources.

Another challenge, *limited access to reliable technology*, may result in homeless individuals using unsecured shared devices. This includes not only logging onto public computers in shelters or public libraries and connecting to public Wi-Fi networks but also using communal mobile phones purchased by and shared among multiple homeless individuals [50]. A few risks may arise from this challenge. For one, simply using such devices in public spaces may put homeless individuals at greater risk of shoulder surfing [14]; similarly, public Wi-Fi networks may be unsecured and open to cyber attacks [9]. For another, forgetting to log out of such shared devices means that other users of the devices can access very sensitive personal information without authorization.

A third challenge, *untrusted relationships*, includes abusive partners or untrustworthy family members. For example, people experiencing IPV may be especially concerned about obfuscating their physical location to avoid harassment, surveillance, and physical abuse. However, beyond intimate relationships, homeless individuals may be concerned about friends and family members having access to their digital services, financial resources, and devices. While close relationships within any population might run similar risks [61], they are particularly precarious for homeless individuals since these accounts and devices can be their lifelines to survival.

The combination of all of these challenges can contribute to a fourth tough times challenge, the sheer *ongoing stress of homelessness*. The intersection of all of these circumstances makes it difficult for homeless individuals to take specific S&P-related action. Specifically, when faced with more pressing issues such as looking for shelter for the night and feeding themselves, S&P may simply not be a priority for homeless individuals. As Sleeper et al. [52] write, "Coping with S&P issues can require mental energy...[but] when people are under stress, thoughtful actions can become difficult".

2.2 S&P and Homeless Service Provision

Although previous research has examined a broad range of S&P challenges faced by homeless individuals, how these challenges specifically manifest within service provision remains underexplored. Past work in HCI [30] has highlighted the critical role service providers play in helping homeless individuals access essential public services, echoing a long tradition in HCI that emphasizes the emotional and technical labor service providers offer to marginalized populations [1, 56, 57]. Gaining a deeper understanding of these interactions is crucial for addressing the unique vulnerabilities that arise when homeless individuals engage with service providers. Prior work has provided a few important insights on client-provider relationships from specific case studies.

On a macro level, data collection of clients' personal information could jeopardize trust between the organization and the clients, as past work has found in food assistance programs [4] and housing services [24]. This is because the parties that provide funding for the service organization, such as both the government and private funders, may have different information needs that override clients' S&P preferences. And on a micro-level, service providers that target specific client communities, such as survivors of IPV and women's shelters [8, 16, 17, 56], or refugees in the United States [51], may act as de facto tech support specialists for clients, even if they are not well-equipped or educated to do so. Havron et al. [20] have proposed formalizing such educational and advice-giving measures as "clinical computer security". Similar to how one might visit a doctor for a medical condition, the authors suggest that consulting with a professional technologist could help IPV survivors navigate difficult S&P scenarios.

2.3 Contribution

In summary, our work differs from prior literature in a few key ways. We build on Sleeper et al. [52], which explored the S&P concerns of people broadly experiencing with homelessness and financial insecurity. Comparatively, our study investigates S&P challenges that emerge specifically when clients and service providers interact. By examining both parties, we surface new insights into how organizational norms and misaligned expectations contribute to S&P concerns. Further, it has been six years since Sleeper et al. published their findings. Since the COVID-19 pandemic, the adoption of digital services has rapidly surged due to social distancing norms, creating a drastically different technological, social, and political environment for our research. Specifically, a societal pivot to telehealth and remote appointments created new technological barriers to clients being able to access services [47].

Additionally, compared to [8], we did not target homeless individuals from specific demographics and experiences, or service providers offering specific services. Instead, we focused on the broad S&P threats and concerns that homeless individuals may face when seeking any public or social service. We find distinct tensions that arise in public, non-specialized service, e.g., routine documentation, inter-agency referrals, and resource limitations. Our findings thus point to immediate action items that service providers, working in any capacity, can address in the absence of S&P clinicians to develop greater trust in their relationship with homeless individuals.

3 Study Design

Drawing upon prior HCI methods [22, 26, 40, 54, 55], we developed a series of storyboards, each covering a critical activity within homeless services. Using these storyboards, we conducted a series of interviews and focus group sessions with people with experiences of homelessness and service provider workers to understand their perspectives, concerns, and desires around S&P challenges in homeless services. (For a deeper dive into the decisions we made throughout the study design and data analysis processes, as well as our reflections on ethical complications and harms from the study, please see the Ethical Considerations section at the end of this paper.)

3.1 Storyboard Development

Given the unique challenges faced by our participants (e.g., literacy, technical education, technology access), and following the methods of [26, 54], we developed a series of easy-to-understand S&P storyboards, based on gender-neutral personas. A storyboard is a "short graphical depiction of a narrative", commonly used within HCI and design research to elicit feedback on how people might interact with a system [55]. Relatedly, comicboarding [22, 40]—a design technique that uses unfinished comic strips as a scaffolding tool—has been employed to gather perceptions and opinions in various HCI contexts. The use of fictional characters can also aid in participants' memory recall and reflection, more so than directly asking participants to share a specific experience. In our study, we followed best practices from previous research with marginalized populations [26], using storyboards as scaffolding to engage participants with diverse levels of reading and technology literacy [22, 40], given that low reading literacy presents a barrier to participation for many unhoused participants [18].

We developed our storyboards through a combination of literature review and iterative group discussions with two service providers, who are unaffiliated with the organizations from which we recruited participants. They serve as the community co-authors of this paper [12]. The storyboard development process started with a review of relevant papers in this domain; from the literature, we collected common cases of S&P challenges within the client-provider relationship in homeless services [5, 13, 26, 52]. The initial set of the storyboards were collected and developed based on the concept of lifeline activities [13], which is a diverse set of activities that require computer and broadband access. We iteratively collected relevant cases from literature and map them across the lifeline activities. Throughout the process, we conducted biweekly discussions sessions with our community co-authors to (1) select, remove or revise certain cases; (2) validate the cases and storyboards based on their domain expertise and lived experiences; and (3) prevent and minimize any potential harms and biases. This rigorous design process aligns with established best practices in HCI literature for engaging with marginalized populations [26, 54].

Through this collaborative process, we identified five critical lifeline activities in client-provider interactions—job search, housing search, health care, education, and social connection—with each storyboard addressing a potential S&P challenge. Each storyboard contains multiple potential S&P threats, vulnerabilities, or attackers, and does not necessarily label either the homeless individual or service provider depicted as being at fault. We summarize each storyboard and the potential associated S&P threats in Table 1. Figure 1 contains one example of the final storyboards we developed and used; the remaining are found in Appendix A.

3.2 Study Protocol

Using the storyboards we developed as scaffolding, we conducted a series of semi-structured interviews and focus groups, both remotely on Zoom and in person, based on participant preference and availability. To help participants feel more at ease about expressing their thoughts, we made sure each session contained only homeless participants or provider participants, never a mix of both. For each session, we started by

Lifeline Activity	**Storyboard Summary**	**Potential Threats**
Job Search [13]	Alex attends a public job fair for homeless individuals at a community center. They give their information to a service provider, who records it with an unencrypted notes app.	Other people attending the job fair might hear Alex saying their information out loud. The lack of encryption in the notes app leaves Alex's information exposed to hackers.
Housing Search [26]	Jordan has been homeless for three months and seeks affordable housing. A service provider uses a shared office computer to fill out a housing application for Jordan and forgets to log out.	Anyone who might be in the service provider's building—client or employee—may be able to access Jordan's information.
Health Care [5]	Taylor, a homeless individual, meets a service provider at a shelter to enroll in health insurance. The service provider helps upload their medication history and current treatments to a Google Drive, but accidentally sets the drive's accessibility to "public".	Anyone on the Internet who has the link to the Google Drive could access Taylor's medical information.
Education [13, 52]	Sam, who is homeless and shares a mobile phone with other homeless individuals, works with a service provider to finance his college tuition. The service provider sends a message about Sam's student loan to the shared phone.	Sam's personal financial information could be seen by the other people with whom he shares the phone. Sam may not be able to access to their bank account if someone loses the shared phone.
Social Connection [13, 52]	Mary is escaping an abusive partner, with whom they used to share a computer. Mary is in contact with a service provider on Facebook to find a new school for their child. In one of their messages to the service provider, Mary reveals the location of their shelter.	Mary's abusive ex-partner can know where Mary is staying; Mary is now in physical danger. The service provider may find out sensitive information about Mary from their Facebook profile, and vice versa.

Table 1: Summaries of the storyboards used in our study session, along with potential associated S&P threats for each one.

asking for consent to participate and video record the session, emphasizing that participants could exit the session at any point and that we were not making judgments of their work or experiences, but only interested in understanding their stories and perspectives. We then gathered participants' demographic information. We also asked service providers about their job responsibilities, and homeless participants about their current housing status and duration of homelessness.

We then proceeded to the main part of the study session. We showed participants one storyboard and asked them to summarize the storyboard to make sure that they comprehended the scenario depicted. We then asked participants to recall any experiences similar to the one in the storyboard, along with follow-up questions such as, *"Did you ever ask questions about why certain personal information was asked of you?"*, or *"Could you tell me about any formal training you received to address such S&P issues?"*, for homeless participants and provider participants, respectively. At the end of each storyboard, we asked what changes the participants would make to improve the S&P outcomes of the storyboard's scenario. We then repeated this procedure for all storyboards, counterbalancing the presentation order of storyboards for each study session. In remote sessions, we displayed these storyboards via screensharing; in the in-person session, we distributed paper print-outs of the storyboards for each participant. Interview questions can be found in Appendix B.

3.3 Recruitment

We recruited our participants via a purposive sampling approach [44], targeting both service providers and people with experiences of homelessness (presently or in the past). We first posted flyers in our local community advertising the study. We expanded our recruitment by asking service providers at local and regional service organizations, with whom we had a prior working relationship, to share study details with their organizational mailing lists. These mailing lists included both other service providers and homeless individuals. Provider participants worked at various regional branches of the same larger umbrella organization, which provides services such as community wellness centers, housing support, shelter, client advocacy, and education. Homeless participants had sought services from both these regional branches and other unaffiliated providers in the area. Additionally, to our best knowledge, no homeless participants were directly served by any of the provider participants. This separation was intentional to mitigate perceived power imbalances between the parties. Of the eight providers, five worked across three different branches of the regional network, and three worked at unaffiliated organizations. We visited one of these branches in person and held a study session with homeless clients who were on site during our visit and interested in participating.

We recruited 20 participants: 12 people with experiences of homelessness, and 8 service providers. Service providers were majority White and/or female-identifying; homeless participants covered a broader mix of racial and gender identities; additional participant demographics are in Table 2. We conducted three focus group sessions ranging from two to six participants each, and eight one-on-one interviews. Other than our branch visit, all of the sessions were conducted remotely, although all participants were given the choice to participate remotely or in-person. Due to our participants being part of a hard-to-reach community, we used a mix of both focus groups and interviews to best accommodate their availability. The sessions lasted 52 minutes on average, and we compensated each participant with a gift card worth 60 USD. We chose this amount based on best practices in existing literature [26, 54], not only to compensate participants for their time, but also to accommodate any barriers to participating in our study, such as transportation or internet access costs.

3.4 Data Analysis

We employed a reflexive approach to thematic analysis [6, 7] in analyzing our data. We analyzed the entirety of transcripts, rather than breaking each session down by storyboards, following similar past work in HCI [26, 54]. We first used Otter.ai to transcribe 576 minutes of video recordings from the study sessions. Then, three researchers conducted open coding on all transcripts collaboratively and iteratively, with each transcript being reviewed by at least two people. In between every few transcripts, the researchers had regular meetings to iteratively discuss the coding process, such as challenges and ambiguities. Such discussions are essential in a reflexive thematic analysis approach, as they allow diverse perspectives to collaboratively shape the development of codes and themes via conversation [7, 37]. This initial coding process resulted in a total of 509 codes. The three researchers then met three times to conduct affinity diagramming using Miro, and derived higher-level themes—27 first-level, 11 second-level, three third-level—keeping our three research questions in mind. Finally, the entire research team discussed and finalized these second- and third-level themes, which we present in Section 5. Following recommendations from [37], we did not calculate inter-rater reliability, as reaching consensus is integral to theme development.

4 Findings

We present our findings, grouped around three themes uncovered in our analysis: (1) homeless participants' S&P concerns when interacting with service providers; (2) how service providers considered the S&P of their clients; and (3) participant-envisioned opportunities for aligning client and provider perspectives on S&P. Our three high-level themes closely follow our RQs introduced in Section 1.

Within the first two themes, we present several mirroring sub-themes, with homeless and provider participant perspectives on each, respectively:

- **Interaction characteristics**, or the communication modalities involved in client-provider interactions, and how information is being collected and saved;
- **Client consent and agency**, including how clients might negotiate their S&P with providers;
- **Individual S&P behaviors**, e.g., why homeless participants adopted certain S&P attitudes, and how provider participants remembered to behave securely; and
- **Organizational influences on S&P**, such as the influence of workplace culture on provider participants' S&P.

For the third theme, we present some ways that our participants envisioned addressing the S&P challenges that might arise in the above four sub-themes. These include **bringing up S&P as a point of conversation**, which includes the impact of our storyboarding method on participants' responses; **signals of trustworthiness from providers**, including clearer indicators of training and consent; and **promoting client self-advocacy and independence**, such as helping clients fill out applications for services and manage S&P independently.

Throughout the rest of this paper, we refer to homeless participants with anonymous identifiers beginning with the letter "H", and service providers beginning with the letter "S". Summaries of our findings can be found in Tables 3 and 4.

4.1 Concerns of Homeless Participants (RQ1)

4.1.1 Interaction Characteristics

Homeless participants mentioned names, birth dates, and Social Security Numbers (SSNs) as specific types of information collected. They also mentioned **several communication modalities for interacting with service providers**: meeting in-person at a service provider's organization offices, over the phone, or by SMS or email. Some participants noted that when providers checked in on them in person on the street, their personal information was potentially vulnerable to eavesdropping. H1 said, *"I've seen some people talking to somebody, asking them if they were homeless or they needed help with something, but there were other people around listening to their information, so one person heard it and could tell other people"*. Participants felt that such interactions were typically only used to collect information about themselves.

Homeless participants did not describe specific components of their interactions with service providers much beyond broad caution and tentative distrust. In particular, none of our homeless participants mentioned receiving any sort of technology-related or S&P advice from the service providers they visited, as was the case in prior work [16, 17].

Demographic Characteristic	**Participant Counts or Range**
Race	White (8), Black (2), mixed race (4)
Age	36 to 68 years old (mean = 49.7)
Gender Identity	female (9), male (11)
Housing Status (homeless participants only)	currently unhoused (10), currently housed (2)
Unhoused Duration (homeless participants only)	months (1), years (2), decades (3)
Service Duration (provider participants only)	6 months to 8 years (mean = 4 years)
Job Roles (service providers only)	case management (4), mentorship (1), peer support (4), client intake (1), housing specialist (1)

Table 2: Participants' self-reported demographics. Given the sensitive nature of our context, we present aggregated information. We did not receive full demographic information from six participants.

4.1.2 Client Consent and Agency

The aforementioned sense of caution and distrust may come from the negative experiences the participants had with providers. Multiple participants shared experiences of **service providers giving out their contact information to other organizations without their consent**. H2 recounted an instance where a case worker had shared their medical information with another department without their consent, making them feel betrayed. They found out about the sharing when the other department unexpectedly contacted them. H2 *wished* the interaction had gone as follows:

> *"If you have a caseworker that's really 100% down for you, they should say, 'I see that [H2] is applying for this, but [they're] also eligible for [another service]. With your information that you gave me, you could qualify for something else. Would you like me to go ahead and pass this information on?"'*

H4, a participant in the same study session, lamented: *"I never get asked. [The providers] just take it upon themselves."*

Some participants felt that service providers were not always untrustworthy or adversarial when it came to their S&P, but simply made mistakes or were overworked. In such situations, participants made sure to correct the providers' S&P behaviors. H12 observed a service provider leaving another client's information on their screen during their appointment. Out of precaution for their own information being exposed in the same way to other clients, they asked the provider to log out at the end of the appointment:

> *"When I leave, I ask the lady, 'Are you finished? Can you turn it off? Did you log out?' Because I know if, as she walks away, she lets me see what other people's stuff is on there before she gets to me, then I know she's gonna do it to me, right? Exactly. So I make sure that mine is off before I leave."*

When some participants questioned providers on why certain personal data needed to be collected, though, they felt like they were doing something wrong. They were self-conscious of being labeled as "problematic", "combative", or "out of control" by service providers when they asked questions to better understand data practices (H1-H4). H2 suspected that such labels were shared amongst employees at the same organization, as a warning of sorts, and feared **reputational harms [11] for speaking up**: *"They go around telling all the other staff that you're going to be a problem."*

In other words, participants felt forced to balance not wanting to appear ungrateful for help, with voicing their valid S&P questions. H6 suspected that not giving up certain information meant that they were barred from accessing certain services. They recounted an experience that led them to feel this way:

> *"I would say, 'I would rather not answer that.' ... [The service provider] was like, 'Okay, you're not participating the way I want you to do it. So I'm not gonna give you what you want then.' When you don't want to answer certain things, they put you in a spot where now you're not cooperating so you're not going to get what you wanted to get, like, say, housing or something like that."*

Relatedly, H5 felt that they had to put in extra effort to **present themselves as educated on privacy rights**, so that providers would not take advantage of them:

> *"I know my rights as, you know, HIPAA, or what confidential information I want out or not want out. But unfortunately, not everybody that's at the shelter...has the same knowledge or life experience. You have to advocate [for yourself] when you see that they're...maybe breaking some privacy laws."*

4.1.3 Individual S&P Behaviors

Overwhelmingly, our homeless participants expressed that **S&P was not top of mind, and could be insurmountably costly**. For example, H6 shared that they used a friend's address to receive important documents in the mail, but this left them vulnerable to the friend knowing too much about them. However, they could not afford the costs of both (1) renting a P.O. box to safeguard their mail, and (2) traveling to that P.O. box anyway since their car was broken down. Other participants expressed that S&P was simply not important to think about unless something serious happened to them—echoing [52]—such as identity theft or suffering financial consequences. (Even with such outcomes, participants did not feel particularly pressured to adopt more S&P behaviors, recalling [25]: H5 quipped, *"I'm homeless, so if you're going to try to steal my information to go get a credit card... Yeah, good luck, because you're not going to get far."*)

As for any S&P behaviors homeless participants *did* adopt, they were largely due to suffering negative consequences in the past, or "learning from experience" to protect themselves. For example, a few participants shared that they learned over time not to reveal too much information about themselves to others, so that they would not be taken advantage of. H1 said that they learned while being incarcerated to *"read [others'] body language"* to decide whether someone could be trusted with their information; seeing "good" and compliant behavior from the providers at their current shelter helped them understand what to watch out for from other providers.

Importantly, though, participants felt that they shouldn't spend energy worrying about being vulnerable with providers. They **didn't want to live with a burden of constant distrust**: *"When you go to a corporate entity or a business to seek assistance, you don't go with the insecurity that they're going to expose your information, right? Why should we worry about that?"* (H10). Or, as H9 puts it, *"If you don't trust them then...I mean, I don't know. I guess you're screwed."*

4.1.4 Organizational Influences on S&P

The issues associated with consent and agency mentioned above extend into homeless participants' broader distrust of service providers to respect their S&P preferences. Participants spoke of perceived disrespect from service providers as a looming factor that clouded all of their interactions.

A majority of homeless participants mentioned that the **sheer number and variance of service providers** that they met and dealt with made it difficult for them to keep track of S&P across all of them. Specifically, the variance in how providers treated them made it difficult for them to trust any of them with their information. For example, H5 told us they were currently in contact with 10 to 15 service organizations, which all had varying levels of professionalism in how they processed and handled their information:

> *"They might give you a tablet to fill out the information, and then it gets, I guess, saved into their computer system. But believe it or not, a lot of other places are very still paperwork-oriented, like on actual paper and pen, which I think is crazy. Social Services itself, they don't have their shit together at all. Like, you send them paperwork, they lose it, and you have to send it over and over and over."*

These experiences caused H5 to rely on only themselves to properly apply for services and access benefits and to **keep their own documentation** of submitted paperwork and applications. H1 and H2 echoed these sentiments, both noting that they took pictures of personal paperwork and kept phone records, respectively.

4.2 Consideration of Client S&P Concerns by Service Provider Participants (RQ2)

4.2.1 Interaction Characteristics

In contrast with homeless participants' experiences of a variety of communication methods, our service provider participants shared unanimously that they tried to **meet their clients in person as much as possible**. S2 told us that because they had built a relationship with their clients and grew to know more about them, they also knew where they spent their time outside of the service provider facilities. As a result, if they wanted to check in on them, they tended not to call, email, or text message, instead preferring to simply visit them in person at their shelter bed or at other facilities they knew their clients visited. Similarly, S8 said they also drove around the streets that their clients frequented to make sure they are okay without making direct contact.

Within the service organizations' facilities, provider participants mentioned **watching out for the S&P of clients** and attempting to educate them on S&P best practices and consequences, echoing [17]. For example, S5 explained how they observed clients using shared computers: *"If I notice [them not logging out], then I'll say, you know, that's really important. Make sure you log out, because the next person sitting here, you know, would have access to your email."*

In the event that providers *did* need to contact their clients via phone, text, or email, they try to **make messages as vague as possible**. For example, S5 shared that if they had to make a phone call, they would simply say, "Hey, this is [S5]. I'm just returning your call." In separate sessions, S5 and S8 both said that they would not identify themselves as a service provider to respect the privacy of their clients, in case a friend or family member overheard the message.

4.2.2 Client Consent and Agency

Again in contrast with homeless participants' experiences, provider participants tended to feel that they create **welcoming environments for clients to give consent and ask questions about data collection**. S5 described how they created a checklist of documents and information they needed to collect from clients, shared that with clients, and allowed them to reflect upon it. Generally, however, after an initial explanation of data collection practices and use cases, S5 said:

Sub-Theme	**Homeless Participant Concerns (RQ1)**	**Provider Participant Considerations (RQ2)**
Interaction Characteristics	Multiple communication modalities—over the phone, text, email, in-person—primarily for taking in personal information; being concerned about eavesdropping during in-person interactions; no mentions of S&P support.	Preference for meeting clients in person as much as possible; if using other modalities, making messages vague to avoid divulging sensitive information; watching out for client S&P during in-person interactions.
Client Consent and Agency	Experiences of providers giving out personal information to others without consent; fear of reputational harms for asking question about data use or S&P; presenting self as more knowledgeable to avoid being taken advantage of.	Creating welcoming environments for clients to give consent and ask question about data use; teaching clients to fill out forms for themselves and protect their S&P independently.
Individual S&P Behaviors	S&P is not top of mind and could be insurmountably costly; not spending energy thinking about S&P to avoid living with a constant burden of distrust in service institutions.	Creating personal reminders and nudges to act more securely, such as logging out of work computers and shredding paperwork; implementing physical S&P measures such as privacy screens and keeping cabinets and offices under lock and key.
Organizational Influences on S&P	Sheer number of and variance across all service providers making it difficult to keep track of S&P and trust any of them; keeping own documentation and personal records so their information doesn't get "lost".	Undergoing extensive vetting procedures from before even being hired, to probationary employment periods, to workplace-imposed physical barriers for S&P, to workplace-mandated S&P trainings.

Table 3: Summary of findings for our *first two themes*: **homeless participants' S&P concerns when interacting with service providers (RQ1)**, and **consideration of client S&P concerns by service provider participants (RQ2)**.

> *"I've never had anybody question further...If you take the time to explain, and you allow them that opportunity to take a look and know that you can print out everything that you've just signed, and you can sit review it, and whatever you need to do... Most people are okay with that."*

S4 also shared how they asked their organization's IT staff questions about how client data was being processed and used, on behalf of their clients:

> *"I tell them what [the IT staff] told me: 'It's just generalized information for the employees that work here in order to know who are they dealing with, and what systems they have. And that information will be kept inside the organization. They do not share it...' This is what they told me. And let's say out of 50 [clients], maybe like 47 [are satisfied]."*

Primarily, however, provider participants typically characterized client agency as **teaching clients to fill out forms for themselves and protect their S&P independently.** Several provider participants mentioned this tactic as a way to (1) divorce themselves from unwittingly absorbing too many personal details about clients, and (2) support clients' sense of independence. For example, S3 told us that the only reason they ever filled out an application for a client was when the client spoke a foreign language and could not read the form:

> *"I felt really uncomfortable because I did not like having to ask certain questions. I didn't even want to know the address...but he could not fill out the form because he didn't know what the words were. So I had to [do it for him]. I don't remember his address [now], but I'm glad I don't... I don't need to know that."*

4.2.3 Individual S&P Behaviors

A frequent S&P practice that provider participants mentioned was simply **remembering to log out of their work computers**, so that digital client data would not be accessible to others in the same physical space. Providers set up various nudges to do so, including setting their computers' screen timeout and account log-in periods to be extremely short. Exemplifying this, S1 expressed their habit of frequently moving their cursor throughout our remote interview to keep themselves logged in, ultimately in vain: *"I just moved [away from the mouse] for one second and it logged out."*

Provider participants also implemented **physical S&P measures** to ensure that client information was protected. S1 used a privacy screen on their laptop monitor to prevent shoulder surfing, and S4 shredded documents as soon as they were finished with them. Multiple participants discussed keeping their environments under physical lock and key, including both file cabinets with sensitive documents, as well as the office rooms themselves; they told us they were the only keepers of those keys. Participants also used such physical separation to have more confidential conversations with clients, closing the door to other employees when necessary.

To keep track of all these practices, participants shared that they created **personal reminders and nudges** to be consistent in their S&P. S7 said they created Post-It Notes for all of the necessary S&P precautions they need to take throughout the day, including locking up their desks and obscuring their physical calendars from other staff; S7 also described habit-stacking behaviors of shredding documents every time they stood up to leave their desk.

4.2.4 Organizational Influences on S&P

From **before they were even hired** as employees of service organizations, multiple provider participants mentioned S&P precautions taken by their employers. Participants shared how the job postings for their positions explicitly stated they should not share client information. Participants also mentioned undergoing multiple rounds of interviews before being deemed trustworthy enough as a candidate, as well as having to sign confidentiality agreements. S3 described how even the geographic location of their office was hidden from them when they had applied for their job, in order to protect the physical safety of clients escaping IPV situations:

> *"I could not find out where [my worksite] was until I had second interview....when I passed that, that's when I was allowed to find out where that place was, because they don't want just anybody walking up there, because somebody could...like this could have been an abusive relationship."*

After being hired, participants described **probationary periods** where they were not allowed to directly interact with clients, but instead had to observe from a distance. S4 believed this period could help habituate clients to a new face in the office and help them trust the new employees more:

> *"[Clients] get to know you from a distance, from seeing you every day for 30 days straight. By the time [the new employee] starts working here, now they kind of know his name, and they can talk to him gradually, because it's a process. It took me almost three to four months before everyone started to talk to me."*

Within the office environment, participants also described **workplace-imposed physical barriers** to promote S&P. For example, S2 mentioned, that within their work office building, there was a separate floor for employees who dealt with clients' medical and health information so that unauthorized employees could not access that data without physically entering the space. S6 and S7 also both shared how their office desks were arranged in a way such that computer monitors were not facing any open doors to prevent shoulder surfing.Participants also described more hands-on administrative involvement in S&P: a few said that administrative and IT staff from "higher up" might perform random checks on their physical workspaces, to make sure that they were properly securing their computers and not leaving sensitive documents out on their desks. S4 mentioned that in their organization, there was one person who was in charge of all IT and S&P affairs and could view all employees' digital work activities:

> *"He can actually know if you put something on the computer that don't belong to you, because I guess he knows everybody that works in each center... Once in a blue moon, I see an email and they advise everybody, 'Yo, be aware that you're suppose to log out if you're not using your computer."'*

Finally, in provider participants' day-to-day operations, they typically had a **blanket trust in their organization's systems and devices** to keep client information secure and encrypted. Many participants said they only accessed and recorded client data on their work computer, which was password-protected, only accessible by them, and *"pretty secure"* (S7). They also mentioned mandatory S&P training sent from administrative and IT staff higher up in the organization, which they felt reinforced a workplace S&P culture. S1 shared that everyone in their organization adopted privacy screens and set their screen timeout period to the shortest duration possible without question. Notably, none of the provider participants mentioned several commonly suggested security measures—e.g., using multi-factor authentication, creating unique and strong passwords, not opening suspicious emails or links, and keeping their devices updated—suggesting that providers may be only focused on S&P measures that result in more interpretable benefits [21,45].

4.3 Envisioned Opportunities for Aligning Client and Provider Perspectives (RQ3)

While the previous two themes demonstrated stark differences in how homeless and provider participants viewed S&P, there were still points of alignment between the two parties. For example, both groups felt it was unacceptable to ever contact each other on social media, no matter how urgent the message. However, because homeless participants did not know of policies or rules explicitly prohibiting this practice, the storyboard heightened their fear of this happening. Meanwhile, provider participants felt that such a rule was so obviously common sense that it didn't need writing down.

This gap in trust and perception led to participants envisioning several design opportunities for clients and providers to be better aligned: **(1)** bringing up S&P as a point of conversation, **(2)** creating clearer signals of trustworthiness from providers, and **(3)** promoting client self-advocacy and independence. We emphasize that these design opportunities were directly mentioned by our participants. Formalizing these *participant-envisioned* opportunities—be it through writing them down into organizational bylaws, or integrating them into official client protocols—may help bridge the gap.

4.3.1 Bringing Up S&P As a Point of Conversation

A common refrain from all participants, both client and provider, was that our workshop sessions themselves caused them to think more critically about S&P. These effects were

Participant-Envisioned Design Opportunities (RQ3)	
Bringing up S&P as a point of conversation	• Storyboards could raise awareness of S&P issues • Workshop questions encourage participants to ask more questions about S&P • Service providers could help clients more directly with S&P issues
Signals of trustworthiness from providers	• More granular, continuous access control and consent-granting procedures • Clearer indicators that service providers receive appropriate training
Promoting client self-advocacy and independence	• Teaching S&P skills applicable outside of the provider-client interaction • Allowing homeless individuals to fill out applications and forms themselves

Table 4: Summary of findings for our *third theme*, **participant-envisioned opportunities for aligning client and provider perspectives on S&P**. This theme corresponds to our RQ3.

twofold. For one, **our storyboards helped raise awareness of certain S&P issues.** The storyboards depicted familiar situations that participants did not realize necessarily "counted" as security and privacy, and participants told us they might feel more aware of recognizing these situations as S&P issues in the future. For example, S3 told us they didn't realize there were so many S&P issues potentially affecting the homeless clients they worked with, once again echoing homeless participants' feelings that they didn't have much to lose [25]:

> *"At first I wondered what the questions [in this interview] could possibly be because I'm thinking, if you're homeless, what do you have that could be hacked into? But then...it's like, of course, there's a lot of things. Even a food stamp or TANF, if you lose that, and somebody else uses it, that's like taking your identity. So when I started seeing the storyboards, then I thought, 'Yes, that makes a lot of sense...' Thank you, because you opened my eyes."*

Similarly, S5 told us that they had not considered that their clients may be sharing a phone with others (and the risks associated with doing so). Instead, they had assumed that the phone numbers that clients provided would be safe to contact. Going forward, they considered asking the client:

> *"When I ask them, 'What is your phone number?', I make the assumption it's [solely] theirs. Maybe it's not a good assumption. Maybe that needs to be a question I ask: 'Is this your own private phone? Is it okay?' I assumed that they would tell me that [on their own]. I probably should maybe ask that, because it could be a breach."*

For another, **the interview questions encouraged participants to ask questions about S&P**. When we asked participants to reflect on authority figures—service providers for the homeless participants, and administrative/IT staff for the provider participants—they frequently told us they would start asking them more questions about S&P in the future. H5 said they hoped that people who felt unsure about asking S&P-related questions could participate in support programs to better advocate for their S&P preferences in the future. However, they also felt that **service providers could help them with such S&P issues**, recalling [20]:

> *"I'm all about getting yourself to that confidence, so like, maybe, like, set up some type of therapy and under and try to understand why they don't have that confidence and working towards that. Or there's other organizations that have people, like caseworkers to specifically help advocate for people who can't do it for themselves."*

At the same time, multiple provider participants noted that they *did* already help their clients with S&P and technology-related issues, usually in an ad hoc manner if they saw a client doing something wrong. S4 mentioned that their organization did offer "computer classes" every once in a while, but only one client would show up at a time. Instead, posting signs around shared computers with S&P advice, or breaking up the computer classes into daily quick advice sessions rather than condensing them all into one sit-down session—*"throw the little things out there"*, as S5 put it—could make S&P more approachable and digestible for clients. Directly, formally integrating these helpful behaviors at the organizational level could help clients feel less burdened about asking questions.

4.3.2 Tangible Signals of Trustworthiness

Several homeless participants wanted **more granular access control and consent-granting procedures** when it came to their personal information, and felt that such measures could help them trust providers more. Some felt that providers should take care to ensure a one-to-one relationship between clients and providers: solely the specific case worker that they interacted with should be permitted to access their information, and no one else. As H7 said, *"When I am working with the social workers I expect that only the one that I interact with has a template where she can pull up a document pertaining to housing assistance with my name on it."* And in the event of employee turnover, a few homeless participants felt that they should receive notification that the worker handling their case was leaving, and be asked for consent a second time before their information was transferred to a new employee.

Homeless participants also wanted **clearer indicators that their service providers had the appropriate training** to be dealing with their information. For example, H3 wanted people to receive formal education before being allowed to work as a service provider:

> *"I think the people we give our information to should go to school or something like that because these are lives that people are dealing with, you know? I think it's really important that they know what they're doing....just go through something where there's a vetting situation. "*

H1 felt that the people working in service provider roles should not apply for these jobs if they were not *"100% willing to help people"*. Such perspectives stand in contrast to the extensive vetting procedures and S&P training that our provider participants shared with us, suggesting that even if service providers *are* being trained and selected appropriately, such qualifications should be better communicated to clients.

4.3.3 Client Self-Advocacy and Independence

Echoing Section 4.3.1, providers could further promote clients' S&P by **teaching S&P skills that are applicable outside of the context of the provider-client interaction**. S1, for example, taught clients to use more secure messaging methods, such as turning on encryption in their emails or downloading dedicated messaging apps; while S1 initially intended only to send secure messages to their clients, the encryption or new apps could now protect all of their client's messages. Similarly, S4 and S5 both said they emphasized to their clients to be aware of their surroundings when revealing personal information, not just within the service organization's building, but in other places like train stations or public libraries. S4 advised clients not to speak private information out loud in busy public spaces, but to rather write it down; S5 reminded clients to constantly log out of shared devices.

Despite these positive interactions, people experiencing homelessness may still distrust service provider workers as a whole, due to overwhelmingly negative experiences with other providers. This can make that individual feel uncomfortable sharing their information out loud to fill out applications or intake forms at service organizations. One way to circumvent this issue is to simply **allow homeless individuals to fill out applications and forms themselves**, with supervision or guidance from service providers if necessary.

As noted in Section 4.2.2, some provider participants already ask their clients to fill out forms on their own, partially to avoid inadvertently learning sensitive information about their clients, but primarily to support their clients' independence. S3, the provider who helped out a client with a language barrier, said they typically sat alongside a client filling out a form and answered the client's questions. However, they would not fill out the information or take action *on behalf* of the client; instead, S3 said, *"I could get [my client] into the system to look for housing, but she had to look herself. That's training someone not to be helpless."* A secondary provider benefit to supporting client independence was that they did not have to be liable for potential negative outcomes: S7 shared that while they helped their clients create budgets, they avoided accessing clients' actual financial or banking information out of liability fears:

> *"A lot of [my client work] has to do with budgeting their once-a-month payment from Social Security. I typically steer clear of having anything to do with, like, the actual banking, because that's a slippery slope...you don't want any blame. With finances, people are quick to accuse others of things."*

5 Discussion

In this discussion, we hypothesize about the factors contributing to the mismatches between clients and providers, including structural and policy forces. We also provide directions for future work as relevant.

5.1 Mismatches in Client/Provider Security and Privacy Priorities

We uncovered much evidence of a set of mismatches in S&P priorities between homeless participants and provider participants. Below we offer a few possible explanations that emerged from our data.

First, the power differential between clients and providers might contribute to these mismatches. Our homeless participants frequently mentioned that they felt like they could not negotiate consent for giving up personal data when interacting with service providers. They worried that they might suffer reputational harms from refusing to give up certain information, e.g., the service provider might tell colleagues that they were a problematic or combative client. More gravely, they were concerned they might be denied access to services if they did not give up their personal information. On the other hand, while our provider participants understood why clients might not trust them, they did not actively refer to themselves as being in a position of power over their clients during our study sessions. This may explain why, even though all of our provider participants felt like they created welcoming and open environments where clients were free to say no, all of our homeless participants perceived the situations differently.

Second, a lack of transparency about organizational practices may contribute to further mistrust. As discussed in Section 4.3.2, homeless participants wanted tangible indicators of control over their personal information, and that service providers were properly trained to handle their information. To them, consent and access control meant being granularly asked if it was okay for the service provider to record certain information about them, and to be asked again in the event of employee turnover or organizational restructuring. "Appropriate training" meant being able to see the certificates and qualifications that service providers had earned as proof that they were qualified. Conversely, our provider participants typically only described asking for consent one time, at intake, and spoke of internal organizational vetting procedures and trainings, to which homeless individuals would not be privy.

Finally, structural forces outside of the control of both homeless individuals and service providers may contribute further to these mismatches. Service providers—many of whom are funded by local or state governments—may be required to follow information protocols and service provision priorities mandated by those entities, which, as noted in Section 2.2, can override the concerns and preferences of their clients [4]. Federal surveillance of marginalized communities further takes agency away from them; homeless individuals are often required to offer extremely sensitive information for the exchange of access to essential public services [26]. As Virginia Eubanks documents in *Automating Inequality* [15], mass-collection of personal data at state-level public assistance offices is now standard practice, and sharing this data to make decisions about services across offices—i.e., "coordinated entry"—is championed at the federal level by the United States Interagency Council on Homeless and the U.S. Department of Housing and Urban Development.

5.2 Opportunities for Alignment in Priorities

Unfortunately, the individual service providers who simply want to help their communities are forced to navigate this ecosystem. Without structural or policy-level interventions, they are forced to navigate conflicting demands from regulatory bodies and their clients. To truly address these systemic issues, we need higher-level policy interventions to realign priorities. Below we offer a few concrete stakeholder-based recommendations, as a first step, to bridge the mismatches.

5.2.1 Recommendation for Service Providers

First, as discussed in Section 4.3.3, clients expressed a strong desire for clear and tangible indicators of how their personal data is handled. This suggests that providers could develop public-facing S&P reports that explain what data is collected, how it is stored, and who has access, using accessible language and visuals. "Know Your Rights"[1] (KYR) campaigns have frequently appeared in other domains, including health care, employment, immigration, and voting. Within the United States, for example, the Equal Employment Opportunity Commission has issued a standardized KYR poster summarizing laws related to employment discrimination and ways for workers to file complaints[2]. Within homeless services provision, a KYR poster might detail the rights that clients have to giving or withholding personal information, and how to submit complaints if they either feel unduly pressured to give up information or uncomfortable with how their provider is handling their data. Such a poster should be prominently displayed in both the providers' offices and throughout the service organizations' physical site, as a first step to help clients self-advocate.

Second, as suggested in 4.3.1, in addition to offering simple explanations of how clients' data is handled, service providers can also amplify details about organizational S&P and data use procedures and the complex environment in which providers operate. Highlighting these factors can help stakeholders, such as homeless clients and policymakers, better understand the multifaceted constraints providers face in delivering care. For example, they could create public-facing reports that outline their data use procedures in simple, accessible language. Sharing anonymized case studies of real-world provider-client interactions and specifically framing them as S&P issues could also offer a deeper, more relatable understanding of these dynamics and the intricate balance providers must maintain in their roles.

Finally, inspired by the opportunities identified by our homeless participants in Section 4.3.2, implementing "continuous" authentication procedures with auditable consent trails of data access, could also reinforce trust between the two parties, especially when service providers change personnel.

5.2.2 Recommendations for Organizational Leaders and Policymakers

First, Section 4.3.2 revealed that clients trust providers more when they can verify their qualifications. Organizations could invest in standardized training and certification programs focused on S&P competencies. In particular, standardization across organizations can also help *clients* gauge appropriate expectations for their interactions with providers. Importantly, provider trainings about S&P should highlight how power differentials between themselves and clients may mean that clients feel compelled to give up too much information about themselves.

Second, as we've shown in our findings, providers spent lots of efforts in practicing myriad forms of invisible labor and emotional care [1,56,57] for their clients when managing S&P related challenges, such as managing emotions, building trust, and addressing clients' emotional needs. For example, as we reported in Section 4.2.1, provider participants drove around streets where they knew their clients frequented to quietly confirm clients' physical wellbeing, and also observed

---

[1] https://www.aclu.org/know-your-rights

[2] https://www.eeoc.gov/poster

clients' S&P behaviors when they used organizational computers. These efforts are critical for managing S&P challenges, yet they frequently go unrecognized in formal evaluations. The emotional toll of this labor, including risks of burnout and compassion fatigue, underscores the need to value these contributions. Towards this end, organizations should consider developing acknowledgment programs that highlight providers' emotional labor and expanding performance metrics to explicitly assess and reward emotional care practices in managing S&P-related challenges.

Finally, across our findings, we observed that clients expressed expectations for S&P that diverge from existing organizational processes and policy assumptions. In particular, as we found in Section 4.3.1, provider participants often did not previously formally associate many of the client issues they dealt with as S&P; only after seeing our storyboards did these participants become more convinced that they had past experience with S&P, or that their clients faced S&P issues at all. Organizations could engage in similar co-design activities with affected communities to ensure that people's lived experiences are integrated into data protection frameworks, supporting more responsive and equitable service provision.

6 Conclusion

We created a set of storyboards to represent S&P challenges that can arise when homeless individuals and service providers interact. We used these storyboards to scaffold a series of interviews and focus groups with 12 homeless individuals and 8 service providers in the Northeastern United States, to explore the S&P challenges that might arise within client–provider relationships in homeless services. We uncovered evidence of a set of mismatches in S&P priorities between clients and providers, possibly owing to power differentials between clients and providers and a lack of transparency about the S&P practices of homeless service organizations. Encouraging conversations about S&P between clients and providers, demonstrating clearer signals of trustworthiness from providers, and promoting clients' self-advocacy and independence could engender greater trust in S&P between the two parties.

Ethical Considerations

This work explores the security and privacy (S&P) experiences of individuals experiencing homelessness and their interactions with service providers. The primary stakeholders include (1) individuals with lived experience of homelessness who participated in interviews or focus groups, (2) service providers who discussed internal practices and organizational constraints, and (3) non-participant clients whose experiences may be indirectly represented. Potential harms included retraumatization, breaches of privacy or confidentiality, misrepresentation of marginalized voices, and reputational harm to service organizations.

The study was approved by our institutional IRB. However, beyond this approval, given the vulnerability of participants and the sensitive nature of the discussion, we took great care to implement rigorous safeguards throughout our research design, data collection, and analysis. Below, we discuss in detail how we considered potential harms and relevant mitigations throughout our research; evaluate the trade-offs of our decisions; and provide recommendations for future work.

Recruitment and Compensation. Participants were recruited through community organizations and public postings at unaffiliated sites. All participants were informed that participation was voluntary, that they could skip any questions or withdraw at any time, and that their involvement would not affect access to any services. Each participant received a $60 gift card, consistent with our IRB-approved protocol and in line with best practices for research involving individuals experiencing homelessness (e.g., [52]. This amount was selected to fairly compensate participants for their time, expertise, and associated burdens such as transportation, logistical coordination, and emotional labor. Compensation was standardized across participant roles and was not contingent on the length or content of the session. No service provider participants were involved in the recruitment or interviewing of homeless participants, and we explicitly communicated that the research was independent of any service-providing institution to mitigate potential perceptions of coercion.

Session Structure and Consent. Interviews and focus groups were conducted either via Zoom or in person, depending on participant preference and accessibility needs. Prior to each session, we obtained informed consent and reiterated the option to stop or skip any portion of the discussion. Participants were told they could withdraw at any time without penalty and were offered follow-up resources, including crisis support lines and informational pamphlets.

To support discussion of abstract and emotionally sensitive topics, we developed storyboard scenarios grounded in real-life service contexts. These were co-designed and vetted with two experienced service providers unaffiliated with the organizations studied. One scenario included an example of intimate partner violence (IPV), reflecting real and documented concerns in homelessness and housing insecurity. Prior to presenting storyboards, we issued a verbal content warning and offered participants the choice to exit the study at any time they want. At the conclusion of each session, we conducted informal debriefs and provided verbal access to additional support or follow-up if needed.

While we emphasized throughout the sessions that participants could withdraw from the study, we acknowledge that some aspects of our study setup could have led to participants feeling financially compelled to stay in the sessions, even if they were uncomfortable with the subject matter of the storyboards. In particular, those who showed up to the in-person focus group session may have found it particularly difficult to leave after taking the time and effort to travel to the research site. To mitigate these harms in the future, researchers could inform participants of potentially sensitive study contents further ahead of the study sessions (i.e., before participants make plans to travel).

Transcription and Use of Otter.ai. We used Otter.ai to transcribe interviews and focus group audio. Audio was recorded locally and uploaded for transcription under a research account. We selected Otter.ai due to its practical advantages: researcher-controlled uploads and deletions, accuracy at low cost, and minimal third-party exposure, especially compared to hiring external human transcribers. Transcripts were manually reviewed, corrected, and anonymized before analysis. All files were deleted from Otter.ai's platform and destroyed after transcription.

Our process follows practices found in prior USENIX Security work involving at-risk participants (e.g., [53]. However, we acknowledge that in the current climate of artificial intelligence and mass surveillance, the use of Otter.ai presents ethical complications for research purposes. While the company claims that it is compliant with the General Data Protection Regulation (GDPR) in the European Union, news media have reported that it may sell user data to third-parties or disclose personal information to government authorities if compelled[3]. And indeed, Otter.ai's own privacy policy[4] reflects these concerning risks. In future work, researchers should carefully weigh these risks and benefits alongside other transcription methods when executing data analysis plans; they should also explicitly communicate these risks to participants, with clear procedures for revoking consent.

Power Dynamics and Community Collaboration. We acknowledge that our experiences shape our research, and our relative privilege within society provides us with advantages that our study participants do not hold. We are researchers who received training in the United States in human-computer interaction, computer science, communication, and social work; multiple authors have obtained advanced degrees in these fields. Although none of us have experienced homelessness ourselves, some members of the team have worked closely with service provider organizations within our local communities via other research projects.

Specifically, two local service providers worked with us as community partners during the design phase; however, they did not participate in data collection or analysis. This collaboration helped ensure contextual relevance while maintaining independence. We acknowledge that research conducted in partnership with service organizations may influence how participants disclose experiences or concerns, particularly where institutional trust is limited. We addressed this by recruiting a demographically diverse sample across multiple sites and reinforcing our independence from any service provider in all study materials and consent procedures.

By transparently documenting our ethics rationale, tradeoffs, and protections, we aim to inform and support future researchers working with similarly vulnerable communities.

Open Science

Due to the unique vulnerabilities and challenges that our participants face, we are not able to share the full transcripts of our interviews and focus groups. They may reveal personally identifiable information about the participants, even if names are redacted. However, we have shared the full contents of our storyboards and interview protocol in Appendix A and B, respectively. These materials are also available for download on Zenodo at `https://doi.org/10.5281/zenodo.15612259`.

Acknowledgments

We thank our participants for their time and input that shaped this research. This work was generously supported, in part, by a grant from the Carnegie Mellon CyLab Security and Privacy Institute. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not reflect the views of funding agencies.

References

[1] Hunter Akridge, Bonnie Fan, Alice Xiaodi Tang, Chinar Mehta, Nikolas Martelaro, and Sarah E Fox. "the bus is nothing without us": Making visible the labor of bus operators amid the ongoing push towards transit automation. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–16, 2024.

[2] Oghenemaro Anuyah, Karla Badillo-Urquiola, and Ronald Metoyer. Characterizing the technology needs of vulnerable populations for participation in research and design by adopting maslow's hierarchy of needs. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–20, 2023.

[3] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L Mazurek, Dana Cuomo, et al. Sok: Safer digital-safety research involving at-risk users. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 635–654. IEEE, 2024.

[4] Ashley Boone, Carl Disalvo, and Christopher A Le Dantec. Data practice for a politics of care: Food assistance as a site of careful data work. In *Proceedings of the*

---

[3] https://www.politico.com/news/2022/02/16/my-journey-down-the-rabbit-hole-of-every-journalists-favorite-app-00009216

[4] https://otter.ai/privacy-policy

2023 CHI Conference on Human Factors in Computing Systems, pages 1–13, 2023.

[5] Caty Borum Chattoo, Lori Young, David Conrad, and Aras Coskuntuncel. “the rent is too damn high”: news portrayals of housing security and homelessness in the united states. *Mass Communication and Society*, 24(4):553–575, 2021.

[6] Virginia Braun and Victoria Clarke. *Thematic analysis.* American Psychological Association, 2012.

[7] Virginia Braun and Victoria Clarke. Reflecting on reflexive thematic analysis. *Qualitative research in sport, exercise and health*, 11(4):589–597, 2019.

[8] Christine Chen, Nicola Dell, and Franziska Roesner. Computer security and privacy in the interactions between victim service providers and human trafficking survivors. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 89–104, 2019.

[9] Ningning Cheng, Xinlei Oscar Wang, Wei Cheng, Prasant Mohapatra, and Aruna Seneviratne. Characterizing privacy leakage of public wifi networks for users on travel. In *2013 Proceedings IEEE INFOCOM*, pages 2769–2777. IEEE, 2013.

[10] Ishita Chordia, Leya Breanna Baltaxe-Admony, Ashley Boone, Alyssa Sheehan, Lynn Dombrowski, Christopher A Le Dantec, Kathryn E Ringland, and Angela DR Smith. Social justice in hci: A systematic literature review. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–33, 2024.

[11] Danielle Keats Citron and Daniel J Solove. Privacy harms. *BUL Rev.*, 102:793, 2022.

[12] Cynthia E Coburn and William R Penuel. Research–practice partnerships in education: Outcomes, dynamics, and open questions. *Educational researcher*, 45(1):48–54, 2016.

[13] Matt Comi, Sarah Smith, Walter A Goettlich, Perry Alexander, Drew Davidson, and William G Staples. Digital home-lessness: Exploring the links between public internet access, technological capital, and social inequality. *Current Sociology*, 72(1):65–82, 2024.

[14] Malin Eiband, Mohamed Khamis, Emanuel Von Zezschwitz, Heinrich Hussmann, and Florian Alt. Understanding shoulder surfing in the wild: Stories from users and observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 4254–4265, 2017.

[15] Virginia Eubanks. *Automating inequality: How high-tech tools profile, police, and punish the poor.* St. Martin’s Press, 2018.

[16] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. " is my phone hacked?" analyzing clinical computer security interventions with survivors of intimate partner violence. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–24, 2019.

[17] 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):1–22, 2017.

[18] Lenin C Grajo, Sharon A Gutman, Hannah Gelb, Katie Langan, Karen Marx, Devon Paciello, Christie Santana, Ashley Sgandurra, and Krysti Teng. Effectiveness of a functional literacy program for sheltered homeless adults. *OTJR: Occupation, Participation and Health*, 40(1):17–26, 2020.

[19] Rosanna E Guadagno, Nicole L Muscanell, and David E Pollio. The homeless use facebook?! similarities of social network use between college students and homeless young adults. *Computers in Human Behavior*, 29(1):86–89, 2013.

[20] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. Clinical computer security for victims of intimate partner violence. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 105–122, 2019.

[21] Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, NSPW ’09, page 133–144, New York, NY, USA, 2009. Association for Computing Machinery.

[22] Alexis Hiniker, Kiley Sobel, and Bongshin Lee. Co-designing with preschoolers using fictional inquiry and comicboarding. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 5767–5772, 2017.

[23] Naja Holten Holten Møller, Trine Rask Rask Nielsen, and Christopher Le Dantec. Work of the unemployed: An inquiry into individuals’ experience of data usage in public services and possibilities for their agency. In *Proceedings of the 2021 ACM Designing Interactive Systems Conference*, pages 438–448, 2021.

[24] Naveena Karusala, Jennifer Wilson, Phebe Vayanos, and Eric Rice. Street-level realities of data practices in homeless services provision. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), nov 2019.

[25] Anastassija Kostan, Sara Olschar, Lucy Simko, and Yasemin Acar. Exploring digital security and privacy in relative poverty in germany through qualitative interviews. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 2029–2046, 2024.

[26] Tzu-Sheng Kuo, Hong Shen, Jisoo Geum, Nev Jones, Jason I Hong, Haiyi Zhu, and Kenneth Holstein. Understanding frontline workers' and unhoused individuals' perspectives on ai used in homeless services. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–17, 2023.

[27] Christopher A Le Dantec. Feature life at the margins: assessing the role of technology for the urban homeless. *interactions*, 15(5):24–27, 2008.

[28] Christopher A Le Dantec, Jim E Christensen, Mark Bailey, Robert G Farrell, Jason B Ellis, Catalina M Danis, Wendy A Kellogg, and W Keith Edwards. A tale of two publics: Democratizing design at the margins. In *Proceedings of the 8th acm conference on designing interactive systems*, pages 11–20, 2010.

[29] Christopher A Le Dantec and W Keith Edwards. Designs on dignity: perceptions of technology among the homeless. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 627–636, 2008.

[30] Christopher A Le Dantec and W Keith Edwards. The view from the trenches: Organization, power, and technology at two nonprofit homeless outreach centers. In *Proceedings of the 2008 ACM conference on Computer supported cooperative work*, pages 589–598, 2008.

[31] Calvin A Liang, Sean A Munson, and Julie A Kientz. Embracing four tensions in human-computer interaction research with marginalized people. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 28(2):1–47, 2021.

[32] Michael Massimi, Jill P Dimond, and Christopher A Le Dantec. Finding a new normal: the role of technology in life disruptions. In *Proceedings of the acm 2012 conference on computer supported cooperative work*, pages 719–728, 2012.

[33] Jessica McClearn, Rikke Bjerg Jensen, and Reem Talhouk. Security patchworking in lebanon: Infrastructuring across failing infrastructures. *Proceedings of the ACM on Human-Computer Interaction*, 8(CSCW1):1–26, 2024.

[34] Nora McDonald, Karla Badillo-Urquiola, Morgan G Ames, Nicola Dell, Elizabeth Keneski, Manya Sleeper, and Pamela J Wisniewski. Privacy and power: Acknowledging the importance of privacy research and design for vulnerable populations. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–8, 2020.

[35] Nora McDonald and Andrea Forte. The politics of privacy theories: Moving from norms to vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2020.

[36] Nora McDonald and Andrea Forte. Privacy and vulnerable populations. In *Modern socio-technical perspectives on privacy*, pages 337–363. Springer International Publishing Cham, 2022.

[37] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice. *Proceedings of the ACM on human-computer interaction*, 3(CSCW):1–23, 2019.

[38] D Keith McInnes, Alice E Li, and Timothy P Hogan. Opportunities for engaging low-income, vulnerable populations in health care: a systematic review of homeless persons' access to and use of information technologies. *American journal of public health*, 103(S2):e11–e24, 2013.

[39] Leticia R Moczygemba, Lauren S Cox, Samantha A Marks, Margaret A Robinson, Jean-Venable R Goode, and Nellie Jafari. Homeless patients' perceptions about using cell phones to manage medications and attend appointments. *International Journal of Pharmacy Practice*, 25(3):220–230, November 2016. _eprint: https://academic.oup.com/ijpp/article-pdf/25/3/220/36595804/ijpp12321.pdf.

[40] Neema Moraveji, Jason Li, Jiarong Ding, Patrick O'Kelley, and Suze Woolf. Comicboarding: using comics as proxies for participatory design with children. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 1371–1374, 2007.

[41] Collins W Munyendo, Yasemin Acar, and Adam J Aviv. "desperate times call for desperate measures": User concerns with mobile loan apps in kenya. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 2304–2319. IEEE, 2022.

[42] National Center for Homeless Education. The mckinney-vento definition of homeless, 2019. Accessed: September 12, 2024.

[43] Office of Community Planning and Development. The 2023 annual homelessness assessment report (ahar) to congress. Technical report, U.S. Department of Housing and Urban Development, 2023.

[44] Lawrence Palinkas, Sarah Horwitz, Carla Green, Jennifer Wisdom, Naihua Duan, and Kimberly Hoagwood. Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and policy in mental health*, 42, 11 2013.

[45] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. A comprehensive quality evaluation of security and privacy advice on the web. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 89–108, 2020.

[46] Jahmeilah Roberson and Bonnie Nardi. Survival needs and social inclusion: Technology use among the homeless. In *Proceedings of the 2010 ACM conference on Computer supported cooperative work*, pages 445–448, 2010.

[47] Natalia M Rodriguez, Alexa M Lahey, Justin J MacNeill, Rebecca G Martinez, Nina E Teo, and Yumary Ruiz. Homelessness during covid-19: challenges, responses, and lessons learned from homeless service providers in tippecanoe county, indiana. *BMC Public Health*, 21:1–10, 2021.

[48] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. " privacy is not for me, it's for those rich women": Performative privacy practices on mobile phones by women in south asia. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 127–142, 2018.

[49] Shruti Sannon and Andrea Forte. Privacy research with marginalized groups: what we know, what's needed, and what's next. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2):1–33, 2022.

[50] Anne B Shlay and Peter H Rossi. Social science research and contemporary studies of homelessness. *Annual review of sociology*, 18(1):129–160, 1992.

[51] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. Computer security and privacy for refugees in the united states. In *2018 IEEE symposium on security and privacy (SP)*, pages 409–423. IEEE, 2018.

[52] Manya Sleeper, Tara Matthews, Kathleen O'Leary, Anna Turner, Jill Palzkill Woelfer, Martin Shelton, Andrew Oplinger, Andreas Schou, and Sunny Consolvo. Tough times at transitional homeless shelters: Considering the impact of financial insecurity on digital security and privacy. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2019.

[53] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, and Rahul Chatterjee. " 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)*, pages 105–122, 2023.

[54] Ningjing Tang, Jiayin Zhi, Tzu-Sheng Kuo, Calla Kainaroi, Jeremy J Northup, Kenneth Holstein, Haiyi Zhu, Hoda Heidari, and Hong Shen. Ai failure cards: Understanding and supporting grassroots efforts to mitigate ai failures in homeless services. In *The 2024 ACM Conference on Fairness, Accountability, and Transparency*, pages 713–732, 2024.

[55] Khai N Truong, Gillian R Hayes, and Gregory D Abowd. Storyboarding: an empirical determination of best practices and effective guidelines. In *Proceedings of the 6th conference on Designing Interactive systems*, pages 12–21, 2006.

[56] Emily Tseng, Mehrnaz Sabet, Rosanna Bellini, Harkiran Kaur Sodhi, Thomas Ristenpart, and Nicola Dell. Care infrastructures for digital security in intimate partner violence. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–20, 2022.

[57] Nervo Verdezoto, Naveen Bagalkot, Syeda Zainab Akbar, Swati Sharma, Nicola Mackintosh, Deirdre Harrington, and Paula Griffiths. The invisible work of maintenance in community health: challenges and opportunities for digital health to support frontline health workers in karnataka, south india. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1):1–31, 2021.

[58] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L Mazurek, Manya Sleeper, and Kurt Thomas. Sok: A framework for unifying at-risk user research. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 2344–2360. IEEE, 2022.

[59] Jill Palzkill Woelfer and David G Hendry. Homeless young people's experiences with information systems: Life and work in a community technology center. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 1291–1300, 2010.

[60] Jill Palzkill Woelfer and David G. Hendry. Homeless young people on social network sites. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, page 2825–2834, New York, NY, USA, 2012. Association for Computing Machinery.

[61] Yuxi Wu, W Keith Edwards, and Sauvik Das. Sok: Social cybersecurity. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1863–1879. IEEE, 2022.

A Storyboards

We include the five storyboards we developed for our study, shown in Figure 2. They depict potential security and privacy situations that people experiencing homelessness may come across when interacting with social service providers. The presentation order of the storyboards was randomized throughout our study sessions.

B Interview Protocol

B.1 Questions for Homeless Participants

For each storyboard, we asked the following questions:

1. Take a moment to read through these drawings. Could you summarize in your own words what the storyboard is about?
2. Have you ever been in a similar situation with service providers? Can you tell me about it?
3. What information did you provide to the service provider? Did you consider that information private?
4. How do you think the information you provided to the service providers was being used?
5. Did you have any concerns about the safety of your information?
6. What would happen if this information was leaked?
7. Looking back at this storyboard, is there anything you would change about the interaction between [storyboard character] and the service provider?

We followed up with additional questions as relevant throughout each storyboard:

1. Did you experience cases where you were not willing to share information or were concerned about how the information stored and used?
2. How did the service provider respond to your concerns? Were you satisfied with their responses?
3. What kinds of measures could help you feel more comfortable about sharing your personal information?

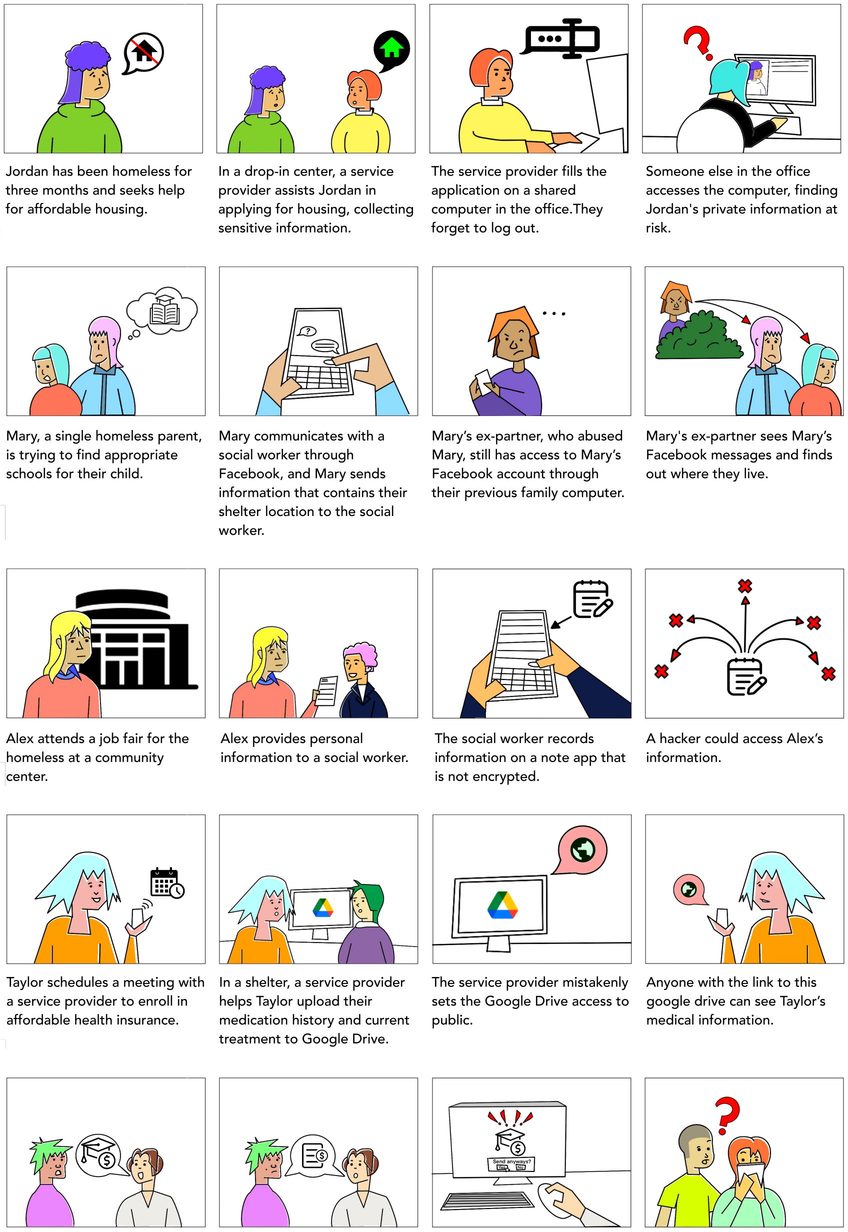
B.2 Questions for Provider Participants

For each storyboard, we asked the following questions:

1. Take a moment to read through these drawings. Could you summarize in your own words what the storyboard is about?
2. Have you ever been in a similar situation with clients? Can you tell me about it?
3. What kinds of personal information do you collect from clients in these situations? Do you consider that information private?
4. Could you tell us about the ways you use, manage, and store this information?
5. What do you think about the safety of these methods?
6. Are there cases where you would need to share this information with others?
7. What would happen if this information was leaked?
8. Looking back at this storyboard, is there anything you would change about the interaction between [storyboard character] and the service provider?

We followed up with additional questions as relevant throughout each storyboard:

1. Did you experience cases where clients were not willing to share information or were concerned about how the information they shared is stored and used?
2. How did/would you answer? Are clients satisfied with your responses?
3. Are there other measures you might take to help clients feel more comfortable about sharing personal information? Do you get training to handle these situations?
4. What kind of training did you get about handling private information and ensuring security?
5. Were you asked any questions during your job interview about handling private information?



Jordan has been homeless for three months and seeks help for affordable housing.

In a drop-in center, a service provider assists Jordan in applying for housing, collecting sensitive information.

The service provider fills the application on a shared computer in the office.They forget to log out.

Someone else in the office accesses the computer, finding Jordan's private information at risk.

Mary, a single homeless parent, is trying to find appropriate schools for their child.

Mary communicates with a social worker through Facebook, and Mary sends information that contains their shelter location to the social worker.

Mary's ex-partner, who abused Mary, still has access to Mary's Facebook account through their previous family computer.

Mary's ex-partner sees Mary's Facebook messages and finds out where they live.

Alex attends a job fair for the homeless at a community center.

Alex provides personal information to a social worker.

The social worker records information on a note app that is not encrypted.

A hacker could access Alex's information.

Taylor schedules a meeting with a service provider to enroll in affordable health insurance.

In a shelter, a service provider helps Taylor upload their medication history and current treatment to Google Drive.

The service provider mistakenly sets the Google Drive access to public.

Anyone with the link to this google drive can see Taylor's medical information.

Sam works with social workers to seek for bank loans to pay his tuition.

Sam provides his personal information to social workers.

A Social worker sends message to Sam's phone which is also shared by other homeless people.

Sam's personal information might be seen by other homeless individuals.

Figure 2: The five storyboards we developed for our study.