Bridging Barriers: A Survey of Challenges and Priorities in the Censorship Circumvention Landscape

Diwen Xue*† Anna Ablove*† Reethika Ramesh† Grace Kwak Danciu‡ Roya Ensafi†
†University of Michigan ‡Independent

Abstract

The ecosystem of censorship circumvention tools (CTs) remains one of the most opaque and least understood, overshadowed by the precarious legal status around their usage and operation, and the risks facing those directly involved. Used by hundreds of millions of users across the most restricted networks, these tools circulate not through advertisements but word-of-mouth, distributed not through appstores but underground networks, and adopted not out of trust but from the sheer necessity for information access.

This paper aims to elucidate the dynamics and challenges of the CT ecosystem, and the needs and priorities of its stakeholders. We perform the first multi-perspective study, surveying 12 leading CT providers that service upwards of 100 million users, combined with experiences from CT users in Russia and China. Beyond the commonly cited technical challenges and disruptions from censors, our study also highlights funding constraints, usability issues, misconceptions, and misbehaving players, all of which similarly plague the CT ecosystem. Having the unique opportunity to survey these at-risk CT stakeholders, we outline key future priorities for those involved. We hope our work encourages further research to advance our understanding of this complex and uniquely challenged ecosystem.

1 Introduction

Recent decades have seen a significant escalation of censorship efforts by nation-state actors around the world. In the first half of 2023 alone, Access Now reported over 80 instances of Internet access disruptions across 21 countries [13]. Notorious among these is China's Great Firewall (GFW), which has been filtering access to foreign websites for over two decades [5, 34, 54]. Similarly in Iran, the national censor routinely targets social media platforms, particularly during times of political unrest [4, 15, 16]. In Russia, the implementation of the "Sovereign Internet" law has further restricted access to international news and media during the Ukraine war [55, 56, 77], effectively creating information bubbles that have isolated the country from the global Internet.

In response to escalating censorship measures, users in affected regions have been actively seeking methods to circumvent censorship. Starting with plain HTTP proxies, VPNs, and website mirrors, the ecosystem of circumvention tools (CT) has evolved along with the advancements in censors' detection and filtering techniques, leading to an ongoing arms race [27, 66]. Over the past decade, on-the-ground developers and academic researchers have developed various dedicated CTs (e.g. [7, 11, 12]) that are specifically designed to facilitate access in censored networks.

Despite these past efforts, challenges remain within the CT ecosystem. While much of the previous research has focused on designing circumvention protocols with evolving obfuscation strategies [2, 19, 24, 35, 36, 45, 70, 76, 79], simply having a technically sound obfuscated protocol does not automatically resolve the difficulties faced by users in censored regions. A gap exists in translating academic state-of-the-art CT research into practical, operational deployments that are available to on-the-ground users and address their actual needs. Even for those tools that are deployed, questions remain unanswered: How do users find about CTs in a sociopolitical environment determined to prevent firewall circumvention? How do CT providers sustain their service? How do factors like risk, trust, and cultural or regional specifics affect the operation and usage of CTs? Gathering feedback from those directly involved in circumvention could help with the relevance of academic research and assist those on-the-ground in creating more efficient and resilient circumvention solutions.

The CT ecosystem differs fundamentally from those of other privacy and security-focused tools. For one, the area of censorship circumvention is inherently adversarial, with CTs often operating in environments where censors actively disrupt their access. Moreover, unlike typical software engineering with iterative development-feedback loops, the development of CTs is often an ad-hoc process, hindered by limited communication between providers and their users. Due to legal and personal safety concerns, providers cannot openly promote their services and techniques, nor can users freely seek, discuss, or give feedback on these tools. These challenges, unique to the CT ecosystem, are often more heightened in the very regions where these tools are most needed.

In this paper, we present the first multi-perspective study to elucidate the challenges and needs of those directly involved

*Joint first authors.

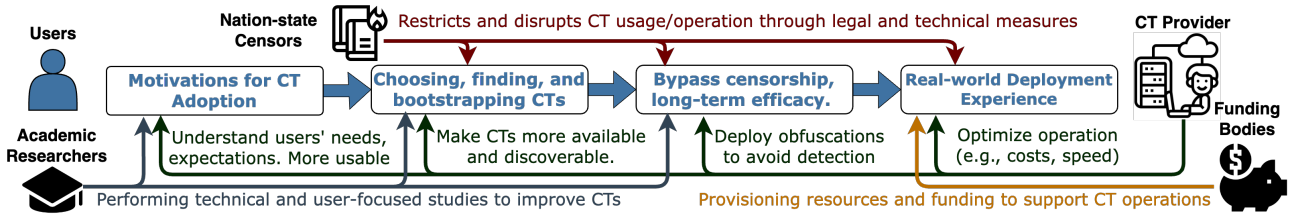

Figure 1: **CT Ecosystems and its Stakeholders**

in censorship circumvention and to identify future priorities as perceived by stakeholders. We interviewed 19 individuals from 12 organizations operating in the CT industry, referred to as "providers" throughout the paper. These organizations, including well-known CT providers such as Psiphon, GreatFire, Jigsaw Outline, ProtonVPN, and OKNO Digital [33, 48, 50, 52, 53], along with others who opted for anonymity, collectively serve upwards of 100 million monthly active users. Through semi-structured interviews, we gathered insights from providers on the technical, operational, and usability issues that drive or impede CT growth, and with inductive thematic analysis, we identified recurring themes that emerged across different phases of CT operation/usage, including:

Discovery & Bootstrapping: How do providers connect with potential users in censored regions, particularly those without existing circumvention methods? What strategies assist the initial CT setup in restricted networks?

Usage & Sustainability: What are the operational challenges for CTs? What is the role of agility and responsiveness in dealing with active adversaries? How do providers sustain their operations and restore services after being blocked?

Risks & Trust: How do participants manage risks in circumvention? In this context, what significance does *trust* hold, and how do providers establish trust with users?

Future Priorities: What do participants identify as the most pressing issues requiring attention, and what priorities should stakeholders, funding bodies, and academia focus on?

Following our interviews with providers, we expanded our study to incorporate perspectives from CT users. We surveyed 24 individuals who live or have lived in Russia or China within the last two and half years, during which they used CTs to bypass the nation-state censorship in these countries. Both provider and user studies involve significant ethical complexities, particularly regarding the sensitivity of establishing connection with on-the-ground individuals with heightened threat models. We are aware of and humbled by the risks our participants took in connecting with us, and we took procedural and technical measures to minimize potential risks, as detailed in § 3.

Our findings reveal multi-dimensional challenges that stakeholders in the CT ecosystem must navigate. Beyond the commonly cited issue of service disruption by censors, our study also highlights funding constraints, usability issues, misconceptions, and misbehaving players, all of which also plague the CT ecosystem. We identified bootstrapping as a critical yet often overlooked issue, which not only complicates CT adoption but also introduces security risks. We found that the limited funding opportunities lead to unintended competition among CT providers, impeding collaboration and sharing of knowledge. We observed a pervasive mistrust within the CT ecosystem, yet users often knowingly expose themselves to potential threats, driven by the sheer need for information access. Based on insights from our participants, we outline several future priorities for stakeholders and suggest actionable recommendations, such as prioritizing user education, coordinated efforts to establish local and regional presence, and facilitating accessible, short-term funding options that support rapid response in times of need.

For the past two decades, the censorship community has been locked in an ongoing arms race with nation-state censors, but progressing beyond this cat-and-mouse game requires a deeper understanding of not only the technical, but also the operational and human-centric aspects of circumvention. Our work identifies a range of issues that, though often less highlighted than technical circumvention research, represent critical points of failure that equally threaten the efficacy and reach of CTs. We hope this exploratory study encourages further research into this space, facilitating the development of more available, usable, and resilient circumvention systems that better address the needs of providers and users on the ground.

2 Background & Related Work

Internet Censorship News, anecdotes, and academic measurement studies collectively suggest a rise in Internet censorship by governments around the world [13,42,59]. Censorship researchers have studied government censorship policies, and in particular, how these policies are enforced through technical means. Inspired from the seminal work on censorship in the 2000s [22, 80], researchers have examined how nation-state firewalls disrupt users' Internet traffic [34, 51, 54], their inferred technical capabilities [41, 69], and their architecture and geographical distribution [26, 74, 77]. Other research has focused on region-specific censorship events during periods of political or social unrest, such as the increased censorship activities in Iran and India near protests or elections [3, 15, 17], and the restrictions on social media and news websites in Russia in the lead-up and course of the Ukraine war [56, 78].

Internet censorship often operates differently across various nation-states. China has consistently enforced a nation-wide web filtering policy for over two decades, using techniques like DNS, SNI, and HTTP keyword filtering [34,54,75]. More recently, in response to the increased use of CTs, the GFW has also been experimenting with new blocking techniques that specifically target these tools, such as blocking fully encrypted CTs based on payload entropy [73]. On the other hand, Russia's approach to Internet censorship has historically been more "decentralized" [55], with the federal communication agency maintaining a blocklist but leaving enforcement and blocking methods to the discretion of individual ISPs. However, since the enactment of the "RuNet" law in 2019, Russia has been moving towards a more centralized censorship model, known as "TSPU" [8, 77]. By 2021, this model allowed Russia to enforce uniform censorship policies across the nation and experiment with new techniques targeting CTs, similar to China's approach [56, 78].

Circumvention Arms Race As censorship measures escalate, users in affected regions are increasingly seeking ways to circumvent these restrictions, leading to an ongoing arms race between censors and circumvention tools (Figure 1). This dynamic is best illustrated in the conflict between GFW and various CTs: censors started by direct blocking of CT websites and public relays, for which CTs deployed website mirrors and unpublished bridges [9]. As censors began exploiting traffic signatures, CTs countered with dedicated obfuscators mimicking mainstream browsers or popular protocols [1, 28, 31]. Censors then used active probing to identify CT servers, leading to the development of probe-resistant defenses [25, 30, 72]. These iterations exemplify the current landscape of the circumvention arms race, where both sides constantly balance between efficacy and expenditure, with new detection and/or obfuscation techniques shifting the costs of various approaches [66].

Prior Qualitative Studies Prior work examined the impact of censorship on information access and users' perception and attitudes towards it. Roberts et al. model censorship as practiced in China not as a ban but as a "tax" on information, positing that if accessing certain information becomes too costly in terms of time and inconvenience, individuals are less likely to seek it out [58]. Their survey among urban Chinese Internet users found that awareness of censorship is low, and the motivation to circumvent it is even lower, largely due to the associated inconvenience. Wang et al. and Kou et al. also explored perceptions of censorship within China [39, 67]. Both studies identified mixed attitudes even among those aware of censorship, with the majority refusing to denounce censorship as purely evil or repressive. They found that attitudes are influenced by demographic background, cultural values, and political inclinations, with a tendency to normalize censorship over time. Shen et al. looked at censorship perceptions across 11 countries outside China, noting significant variations in attitudes towards different types of censored content (e.g. religious vs. political) [64]. More recently, Chen et al. investigated the relationship between censorship and self-censorship [21] and found that perceived necessity of self-censorship amplifies its impact on users' expression desires, which in turn affects their attitudes towards censorship.

On the circumvention side, Kou et al. examined how Chinese Internet users adapt their strategies based on their understanding of the censorship apparatus, such as switching between public and private communication channels based on perceived content sensitivity or communicating in ways believed to be less susceptible to censorship scrutiny [38]. Gebhart et al. surveyed Thai users and found that the way they use CTs can be exposed to potential risks of malware and surveillance, highlighting the need for more informed CT selection [32]. Dai et al. focused on Iranian users, investigating psychological factors influencing CT adoption [23]. They found that attitudes towards media freedom and compatibility with regime ideology significantly impact individuals' decision to use CTs. Contrasting these findings, Mou et al. observed that in China, the usage of CTs is driven not by personal stances or political motivations but by more practical needs, which they attributed to political apathy among Chinese Internet users [46]. More recently, Kwak-Danciu et al. surveyed CT providers to examine their motivations for helping people overcome censorship [40]. They found that the providers were often motivated by a deep-seated belief in the right to access information and a moral imperative to fight back against what they perceived as repression. During the course of our study, Okthanks independently documented insights from eight VPN providers using the Outline tool developed by Jigsaw, revealing the social, technological, and operational challenges they face in circumventing censorship [71].

To the best of our knowledge, we are the first to conduct a study of CT providers augmented by experiences from CT users. Given the CT ecosystem's opaque nature and the heightened risks faced by its stakeholders, our multi-perspective study aims to help security researchers, technologists, funding agencies, and advocates of information freedom better understand the challenges of the current CT ecosystem and highlight areas of priority for concerted efforts.

3 Ethics

Research on censorship and circumvention is inherently sensitive, especially when it involves on-the-ground individuals directly engaged in circumvention efforts. Thus, we followed best practices to mitigate any direct or indirect harm to the participants involved in the study. First, we outlined our survey protocols and sought consultation with senior members of the anti-censorship community. Based on their feedback we finalized our approach. We also cleared our research plan with our university's Institutional Review Board (IRB), who approved our study under Exemption 2.

Our team has a background in performing peer-reviewed censorship measurements in collaboration with in-situ activists for both Russia and China. For our survey's initial recruitment, we leveraged the secure channels established from these previous collaborations. Subsequent recruitment was accomplished with the involvement of Internet freedom NGOs, which facilitated vetted regional meetups to connect us with potential participants. Once the participants were finalized, we provided them an IRB-approved consent form (appended in A.3), which detailed our privacy policy and allowed them complete freedom to abstain from answering any particular question. We opted for asynchronous, text-based interviews for the participants that still reside in censored countries, while offering live and/or in-person options to all other participants (see § 4.3). All live and/or in-person interviews were transcribed in real-time by a team member and the transcriptions were accessible only to select members of the team, following the principle of least-privilege. We additionally emphasize that at no point during the project's duration were audio or video recordings made. Moreover, we ensured to not collect any personally identifiable information during the entire recruitment or interview processes.

4 Methods

We set out to study the perspectives of both providers and users of CTs to understand challenges and dynamics within the ecosystem. To this end, we conducted qualitative interviews with stakeholders from both groups.

4.1 Participant Recruitment

Most of the provider recruitment efforts leveraged our existing connections within the censorship circumvention community, established through either previous collaborations or participation in invite-only events hosted by NGOs or regional meet-ups. To reach additional participants, we used relevant online mailing lists, message boards, and censorship forums. In our recruitment message, we explicitly sought participation from individuals actively involved in the CT industry as developers, distributors, or operators – whom we collectively refer to as "*providers*". We also solicited CT user participants who live/have lived in Russia or China within the last two and half years. We focused on these two countries due to their domestic censorship practices, substantial CT user base, and their sizable diaspora populations. We did not offer any compensation to participants, other than the potential to make an impact assisting academic research on censorship circumvention.

In total, we interviewed 19 individual providers from 12 organizations, among which three focus their operations on Russia, four on China, and the remainder have a global outreach. In addition, we interviewed 24 CT users, including 16 from Russia and 8 from China.

4.2 Interview Protocol

The escalation of censorship practices has significantly driven the demand for effective circumvention tools, yet research on the factors influencing CT adoption and usage lags behind. We designed our interview questions based on our combined experience in censorship research over the past nine years, including both the measurement and analysis of censorship practices and the development of circumvention approaches. These questions cover both the technical and operational aspects of CTs, as well as modes of discovery, usability, and considerations related to risk and trust.

Participants began by answering background questions to describe their involvement in censorship circumvention. For user participants, we asked for their awareness of and reactions to censorship, and motivations driving their circumvention efforts. We then guided both provider and user participants through the journey of discovering and using a CT, followed by a discussion on CTs' operation and sustainability in adversarial settings (e.g., how providers restore services after blocking, and how users react to CTs becoming unavailable). We then explored the perceived risks associated with circumvention efforts and the role of trust in the decision-making processes of both groups. Lastly, we concluded the interviews with open-ended dialogue about future priorities within the CT ecosystem, as identified by the participants. The interview questions can be found in Appendix A.1 and A.2.

Our interviews followed a semi-structured protocol: while we started with a planned script of questions, we also allowed for deviation from the script to clarify statements and explore areas introduced by interviewees. Such an approach balances between maintaining consistency across interviews and allowing novel and unexpected insights to surface [20].

4.3 Interview Procedure

Considering the sensitive nature of research on censorship circumvention, we offered our interview process over multiple modalities: in-person, online via video conference, and asynchronously through text. We extended these options to accommodate any requests for anonymity from our interviewees and to mitigate language and communication barriers, along with the mental loads associated with them.

Each live interview was led by 2-3 researchers from our team, with the lead interviewer following the interview questionnaire and maintaining discussions, while the other(s) actively transcribed in real time. These interviews were not recorded due to privacy and anonymity concerns. All interviews began with the researchers presenting and requesting verbal consent from the interviewee using the IRB-approved consent form. Interviews took between 30 minutes and two hours.

Our text-based interviews included the same set of questions as our synchronous audio/video interviews. For discussion beyond participants' initial responses, we sometimes sent

follow-up text-based questionnaires, but the scope of these follow-up discussions was limited due to the asynchronous nature of these interviews.

4.4 Qualitative Coding and Analysis

Each interview was transcribed by 1-2 researchers in real time. For our analysis, we adopted an inductive, open-coding approach to reflexive thematic analysis [18]. We chose to use reflexive thematic analysis as it aligns closely with our research objectives, which set out to "describe the 'lived experiences' of particular social groups" [65].

To generate initial codes, three researchers randomly selected two interview transcripts each from CT providers and users and collaboratively coded them to develop separate sets of codes for each group. Then, all remaining transcripts were first coded by one primary coder, followed by two secondary coders who independently reviewed the initial coding to identify any missed codes or propose changes where needed. After every three to four interviews, the researchers held meetings to reconcile disagreements until consensus was reached. The iterative process continued until all transcripts had been independently reviewed by at least three researchers.

Following the coding process, we held meetings to collaboratively collate codes into candidate themes and identify emerging themes. As part of our reflexive thematic analysis approach, we then collectively reviewed the candidate themes against the collated codes as well as the original interview responses, refining and collating themes as necessary. Since the researchers reviewed every independently-coded transcript together, we do not present inter-rater reliability [43, 44].

4.5 Limitations

Our provider participants represent some of the most popular CT providers across various regions, yet our user sample may not be fully representative of the global demographic of CT users. For one, many of our user participants were recruited from university mailing lists, which resulted in a demographic that skewed younger and more educated. Moreover, our exploration of user perspectives was limited to Russia and China, as we were not able to safely reach enough respondents from other censored regions, such as Iran or Turkmenistan. However, our study offers concrete insights into the experiences and challenges faced by those directly engaged in censorship circumvention, a group that operates under significant risks yet remains largely understudied in previous work.

5 Results

Based on interviews with both CT providers and users, we present in this section an analysis of the dynamics and challenges in the circumvention ecosystem. The interview questions posed to both groups share many parallels and examining their responses side-by-side can reveal potential (mis)alignments. For this, we structure our results not by separating providers and users, but rather around key themes that surfaced recurrently from our inductive thematic analysis, as shown in Figure 2. Then, for each specific response or quote, we indicate whether it originates from a (**P**)rovider or (**U**)ser.

5.1 Motivations for CT Adoption

The decision to adopt CTs is preceded by the awareness of censorship. While this might seem intuitive, the often subtle and covert practice of censorship can make this recognition less obvious. We ask participants for their perceptions of censorship and to identify the factors that motivated circumvention.

Perception of Censorship Participants associated censorship with emotional distress, such as sadness, frustration, and a sense of being restricted. "*It feels really sad that we have to go through all this, and the isolation worries me.*" (U5) Some users displayed a sense of resignation, accepting censorship and the need for circumvention as "*a daily reality we have to deal with.*" (U14) Other participants expressed anger:

> "Censorship gets you feel irritated! There's no way to actually disable access to anything, everyone mastered proxy use. But it makes hassle, makes your life a bit less comfortable, force you to make small but irritating actions all the time..." (U4)

Regarding motivations for adopting CTs, most participants (n=14) identified practical and entertainment needs that are denied by censorship as primary drivers for seeking circumvention. They emphasized the tangible impacts of censorship on their daily lives, such as being unable to access work-related resources like Github for developers, educational materials like Wikipedia and foreign college applications, and entertainment like gaming or adult websites. Other users (n=7) cited political motivations or personal stances on information freedom. These users turned to CTs to access news or articles censored for political reasons or to advocate for free access to information, and to explore alternative viewpoints that were otherwise unavailable through censored media channels.

Local Alternatives While both Russian and Chinese participants mentioned local websites impacted their CT usage, Chinese participants (n=11) further highlighted the how the existence of local alternatives to blocked services have the potential to make circumvention less urgent or appealing. Especially for services with a social dimension, local alternatives might even be favored as they are more popular among the residents of the censored region:

> "I tried to persuade my parents to use [a CT] but it was not as appealing to them. We set up a family chat on Signal, but it was hard to switch just for three of us while everything else is happening on WeChat. My mom thinks censorship is not good, but she simply doesn't have motivation to circumvent." (U12)

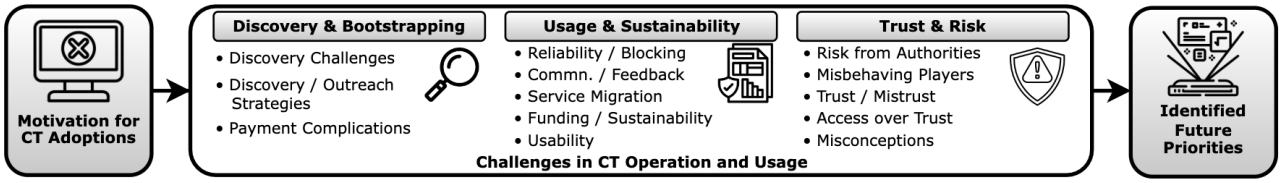

Figure 2: **Structure of the Results Section.** We begin with the motivations behind circumvention efforts, followed by the identified challenges in CT operation and usage, grouped into recurring themes from the interviews. Finally, we highlight future priorities for stakeholders.

More generally, providers also observed that the existence of local alternatives might mitigate the need for circumvention:

> "There is a massive population who are blissfully unaware that outside Internet exists...there's a complete domestic ecosystem that people almost never accidentally stumble upon a website that's censored. How can we make getting past the firewall more appealing? Because no one ever regrets using a CT, it's just that people don't know what they are missing out." (P10)

Perception of Circumvention Several participants pointed out that certain perceptions of CTs, particularly among the non-technical population, can deter their adoption. These perceptions are often fueled by targeted propaganda from the authorities, associating CT usage (VPNs * in particular) with stigmas such as "*VPNs are for people who have things to hide*" (U14), CTs are tools from "*the evil west*" to promote certain narratives, or even that CTs are "*scary, used by terrorists*" (U13). These perceptions can create psychological barriers that demotivate people from adopting CTs.

5.2 CT Discovery and Bootstrapping

In regions where censorship is prevalent, the way potential users discover and connect with CT providers differs significantly from how they might find typical Internet services. As the legal status of CTs often ranges from ambiguous to outright illegal, traditional advertising and outreach channels are often not viable options. In this part of our survey, we discussed with both providers and users how they manage to find each other and bootstrap a circumvention connection.

Censorship Challenges CT Discovery The primary challenge in CT discovery lies in the practice of censorship itself, which often limits access to information about these tools. Surveyed users noted mainstream search engines, a go-to resource in other less adversarial contexts (e.g., western-focused commercial VPNs), are "*outdated as a source for finding CTs*" (U12) due to being blocked themselves. Users from China mentioned that download links for CTs are often not useful for bootstrapping, as these links are regularly censored either by the GFW or by local browsers with built-in URL filters. Additionally, participants mentioned that online forums where CT information might be shared are heavily monitored and censored, with posts frequently being deleted and posters risking consequences (more on risks in § 5.4). U22 on how users discuss CTs by using creative homonyms to stay under the radar, in a continual game of cat-and-mouse with the censors:

> "We refer to providers as 'airports' to evade detection, or 'ladder' (to climb Wall) or 'scientific browsing'. But censors develop extensive lists of such terms, updated mostly manually. [For this,] people have to continuously come up with new words [for CTs]." (U22)

Discovery & Outreach Strategy Censorship against CTs forces both providers and users to adopt a more covert approach to connect with each other. A predominant method, as noted by surveyed users (n=19), is through word-of-mouth – sharing CTs within close-knit circles of friends and family. Recommendations for effective and reliable CTs are passed along in these underground networks. Providers echoed:

> "In China and Iran, there's a massive underground market for circumvention services. Entire Telegram groups dedicated to things like sharing proxy details and selling this information for money." (P10)

U16 shared their experience of obtaining access to CTs through a referral on social media:

> "I paid this anonymous person on WeChat and they provided me with their tools and account info. I don't know if the service has a name. It is not an app I can find in mobile or PC app stores. " (U16)

Participants also mentioned acquiring their CTs through exposure to outside, less censored environments. For example, traveling abroad often allows access to information about CTs that is otherwise censored. Students attending international schools mentioned learning about CTs from their foreign instructors or peers. Maintaining connections with friends and relatives living overseas also creates cross-border information flows for learning about and obtaining CTs.

Another common (n=11) yet somewhat counter-intuitive practice among users is to use one CT as a means to find/bootstrap another CT. In these cases, the initial CT is often a temporary solution, such as a less trusted free VPN or a temporary VPS from a friend. This approach serves mainly

*We note that VPN and CT are not identical: not all VPNs serve as CTs (e.g., enterprise VPN) and not all CTs provide layer 2/3 tunneling (e.g., app-layer proxy). Yet, surveyed users often used the two terms interchangeably.

two purposes: First, users need access to the uncensored Internet to find other, more reliable CTs. Some users mentioned Google as a trusted gateway to finding CTs, and the initial CT is used to unblock such a gateway:

> "I use a free shady VPN from the Chinese app store to then find more reliable tools."(U17) "I can search [CTs] from Google, but first I'll need to have access to Google." (U16)

Moreover, many CTs require a bootstrapping stage before they can provide access. This stage involves authentication or configuration setup, which often cannot be completed under censored network conditions. As such, users may need a secondary CT to complete the bootstrapping process for their primary CT:

> "[Redacted] has a browser extension, which occasionally requires re-authentication. However, the login page itself is blocked. In that case, I need to turn on a third-party VPN to access the login page and authenticate the tool." (U19)

The practice of using CTs to find/bootstrap CTs is also noted by providers:

> "We always wonder how do we reach people without any CTs? Many of our users switched from some other worse CTs. How can these users find us directly [when] obviously our website is blocked?" (P10)

Providers shared their alternative outreach strategies in the absence of traditional advertising channels. Six providers mentioned collaborating with local partners, such as grassroots networks, media organizations, and CT resellers (who bulk purchase access from providers and then sell to individuals). These collaborations allow providers to indirectly reach potential users by leveraging the existing trust and reach of these partners. For example, P2 noted a major influx of new users referred by Russian news websites, which, after being blocked following the start of the Ukraine war, directed their audience to CT services to maintain access.

Payment Complications Users also reported facing difficulties in making payments for their CT services, which is often related more to the challenge of cross-border transactions than to the technical aspects of CTs themselves. For example, some providers only accept payments in USD, which may not be readily accessible to users dealing in local currencies. Additionally, some Russia participants (n=4) discuss how the payment process can be further complicated by economic sanctions, where conventional payment methods like credit cards are restricted. As U8 shared:

> "I often help friends and family pay [for CTs], as Russian banks and cards are blocked under sanction. I think users should be able to pay in some ways... right now they have to circumvent sanctions to actually circumvent censorship." (U8)

5.3 CT Usage and Sustainability

We next discuss the experiences of providers and users in operating and using CTs. Unsurprisingly, a recurrent theme is the issue of CT reliability due to disruption from censors. In regions where censorship is prevalent, authorities often impose restrictions on circumvention methods, through either legal [60–62] or technical measures [14, 25, 72, 73]. Additionally, factors such as usability and funding also affect the adoption and sustainability of the CT ecosystem.

CT Reliability and Blocking The issue of CT services being unreliable is unanimously noted by both providers and users as a primary concern. All surveyed providers recounted instances of their service being blocked in the past. P4 noted on this matter, *"Tools get disrupted all the time in our market. We try to make our tool more available. However, there are cases where authorities still effectively crack down on our service."* Providers servicing Chinese users even postulate that the reliability of their service is often not a matter of the technical capabilities of censors but is rather a choice made by censors, based on non-technical factors such as the CT's popularity or public sentiment.

> "The Chinese censor is a different animal; they are highly organized, well-funded, and work very hard. We manage to remain operational because I sense they intentionally leave a crack...I truly believe that if they decide to shut everyone down, they have the [technical] capability to do so." (P8)

The majority of surveyed users (n=20) also identified CT reliability as the primary issue they faced. Interestingly, their descriptions of CT availability were not in binary terms, i.e., "the CT works" or "the CT does not work". Instead, they described availability as highly contingent on the specific network they were connected to and the time of their connections. Participants noted that their CTs' availability varied greatly as they moved between different networks, e.g., smaller local ISPs that are equipped with less sophisticated Deep Packet Inspection (DPI) or licensed academic or corporate networks. A majority of users (n=12) reported instances of their CTs becoming unavailable during major events, such as election or war.

> "Anytime there's a major conference or significant change in the government, or some negative news that gains public attention, VPN services tend to go down. Circumvention tool users usually expect the tools to fail during these time periods." (U15)

Providers and users agree that censors adopt a strategic, targeted approach to suppress the most popular CT services. "*The problem with CT in China*", as noted by U12, "*is that once the service scales up to a level where it becomes widely known, it attracts the censor's attention for blocking*". Providers additionally shared that the scope of being targeted

by censors extends beyond just the disruption of CT traffic, affecting other operational aspects of their organizations, such as website, email, and API access.

Beyond popularity, a CT's perceived political stance can also make it a higher priority target for censors. P10 alluded to this when discussing what they thought other CTs might be doing:

> "If you seem to be less anti-government than the VPN next door, like by blocking politically controversial websites for your users, maybe they'll crack down on that other VPN first." (P10)

CT providers proactively address the reliability challenge by researching new circumvention techniques or by enhancing the resilience of their existing tools, often through increased redundancy. Four providers specifically mentioned their multi-protocol architecture. This approach involves deploying a variety of transport protocols, enabling their CTs to switch to an alternative protocol in the event of blocking. Moreover, as a more straightforward strategy, providers often resort to rotating IP addresses and servers, particularly when censors are able to fingerprint a CT's traffic.

> "We have a server farm with over 3,000 server instances, rotating IPs faster than the censors block their addresses, with different [rotation] frequency in different targeted countries...still, there have been instances where the censors detected our servers too fast, and [as a result] we lost many users during that period [the shadowsocks blocking incident in 2021 [73]]." (P8)

Following a blocking incident, providers actively work to restore their services. Six providers detailed this process where their R&D teams detect the blocking, reverse-engineer the blocking mechanism, and then develop and deploy countermeasures. For example, P6 shared a specific case [73]: "*Recently, both Iran and China have blocked our tools...we discovered that they were blocking seemingly random traffic. Our countermeasure was to change the output of encryption [to show less entropy].*"

A common thread among providers is the necessity of maintaining communication channels with their users as they recover services from blocking.

> "We need visibility about what happens on the other side...a network of skilled individuals who can test things we are developing. [Without that] we are operating somewhat like shooting in the dark." (P9)

Such communication can range from soliciting help from in-situ users to triangulate the censorship mechanism, to distributing updates once a patch is developed, or simply informing users that a solution is underway. However, maintaining such communication has proven to be one of the most challenging aspects in CT operation.

Communication and Feedback Both providers and users noted the challenge of maintaining a communication and feedback loop, a challenge that is exacerbated during periods of heightened censorship aggression, such as politically sensitive times. These are precisely the moments when effective communication between the provider and the user is most crucial. "*Dictated by the very nature of our work, obtaining feedback is always hard. But it becomes even harder to receive in real time during a blocking [incident], which is crucial for enabling rapid response*" (P8). Seven providers emphasized how the absence of feedback loops complicates their efforts to restore blocked services. P6 and P9 shared that "*knowing how [censorship] is working is hard, as we don't collect metrics on client-side network activities*", and even when they do receive *some* feedback, it's often "*very sparse compared to changes of censorship behaviors*" both geographically and temporally. P11, on how inadequate feedback blocks iterative development:

> "I observe many outages but have little means to diagnose the cause. The available user reports are vague, confused, non-technical, and irreproducible. I try to come up with some general obfuscation, but again, have no way to validate their effectiveness." (P11)

Another challenge highlighted is the difficulties of distributing software patches or updating client-side configurations when the usual communication channels to users are severed due to blocking.

Five providers discussed their existing channels for gathering limited user feedback, such as conducting user surveys, displaying messages on the landing page, addressing support tickets, and communicating through social media posts or press releases. Still, the challenge remains as these channels are either constrained in their bandwidth or limited to uni-directional or asynchronous communications.

Surveyed users (n=4) echoed the communication challenges and expressed the desire for more effective channels to both receive messages from providers and to provide feedback. U7 said "*[I want] More feedback on connection problems. Now, it's hard to understand why the tool is not working - whether the server is down or connection is blocked.*" Participants also asked for a way to share files and logs with providers, which would assist in diagnosing their connection problems.

Providers shared that the disruption from censors is only partially to blame for the lack of communication and feedback. Another significant factor cited is concerns related to privacy.

> "Our philosophy is: by not collecting data, we ensure it cannot be accessed by others. For this we do not collect traffic data." (P8)

Security is often another concern. Providers noted that running services catering to users with heightened threat models can deter outreach or user studies.

> "We had a lot of pushbacks when it comes to talking to users. The more you talk to them, the more they are highlighted. In Turkmenistan there have been stories where police show up to the user's door and ask them to stop using [redacted]" (P5)

Similarly, concerns for their own safety may also deter CT developers located outside censored regions from engaging and conducting tests with in-situ users.

> "We are somewhat limited by concern for anonymity. None of us want any exposure. So when users proposed using their machines in China as vantage points for testing, we didn't dare to do it." (P12)

One surveyed provider highlighted security concerns not in terms of personal risk, but regarding the potential for making their service vulnerable to censors' detection. In response to users requesting more explicit error messages for diagnosing connection problems, the provider explained that providing any feedback at all could inadvertently aid censors with active probing capability to gain information about the server.

> "Our [connection] feedback is not very clear. Users are not able to tell between a revoked access key and network problem. [This way,] we don't leak to a censor anything if they try probing. We always time out instead, which is not ideal for debugging as [a timeout] could also occur due to blocking." (P6)

Service Migration When asked about their strategies in response to their CTs being blocked by censors, user participants mentioned that they would attempt to resolve the issue either by searching online in censorship forums, by reaching out to more tech-savvy friends, or simply by re-attempting connection to a different endpoint if the CT offered multiple options. Two participants expressed a sense of resignation, accepting CT blocking as inevitable during certain time periods, and choosing to just wait "*for the blocking to pass*" (U15,21). Only one participant mentioned directly contacting their CT provider for assistance. The majority of other surveyed users (n=11), however, found themselves in a continual cycle of service migration in order to maintain access to the free Internet.

> "I maintain a lot of back-ups. If one stops working, perhaps the operator gets in trouble or run away, I just switch to another service. (U22) These [CT] services might get shut down [as soon as] next month, so I don't commit to long subscriptions. (U12)"

Participants provided a perspective on why they switch services, believing once a CT is blocked, it is unlikely to recover.

> "They keep becoming unusable, but there's nothing to fix. It just means that the state's filtering system found how to disable them. You just go download a new [CT] because this tool is done. (U4)"

Interestingly, users' frustration over the need to constantly switch to new services is echoed by providers, but from a different perspective: providers find that users often migrate too quickly, leaving little time for providers to implement countermeasures or communicate potential solutions.

> "Once blocked, eventually people believe [redacted] doesn't work anymore. It took us a month to develop [a countermeasure], but the users are not willing to come back because they think it won't work."(P9)

Funding and Sustainability A common (n=5) theme that emerged from our interviews with CT providers is the financial burden associated with running a CT service. Expenses such as renting servers, buying upstream bandwidth, and constantly rotating IP addresses pose a challenge to the sustainability of CT operation. Providers who only offer self-setup CT solutions face this challenge to a lesser extent compared to those who directly operate such services, especially those who offer services free of charge.

> "We have a problem with too many users... It's a free tool. People use it and we don't know how to pay the bills. We always try to support short-term user surges no matter the cost. But once these users start to be active for more than a month, we have to actively try to figure out how to fund it." (P5)

P9, operating a free CT service, shared their frustration on the difficulties in securing funding to support their operation.

> "The bigger problem we face is the lack of resources. Currently, there is no such a thing as a unified entity that recognizes or supports those doing this kind of work. At the end of the day, this operation doesn't pay one cent, and our resources are limited." (P9)

This difficulty in securing funding is a common issue among CT providers. They recognize that operating CTs often means serving users who are unable to pay; as such, they often seek funding from government agencies or organizations. This responsibility of obtaining funding places a burden on providers, who, as P2 mentioned, "*expend a great deal of effort in trying to secure funding*". This process can be complicated by several factors. First, the application for funding can be a lengthy process, which contrasts with the need for rapid response to the changing censorship landscape. P5 shared, "*Censorship is volatile. You can have a user surge of thousands to millions in a single day, while funding agencies are often slow to react.*"

Additionally, providers need to evolve their CT capabilities to stay matched in the ongoing arms race against censors, yet they often struggle to explain their specific needs to justify funding, such as the costs involved in researching and developing new circumvention solutions. The funding can also be insufficient to cover long-term operational costs. One participant shared their experience of having to "*constantly create*

new projects just to get funding" (P4). The funding can also come with restrictive conditions, such as region-specific funds that limit their use to support users only from a certain area.

Providers raised a concern about the limited funding opportunities creating an unintended competition among CT providers, which can have negative effects on the ecosystem.

> "There's a competition mentality, particularly in competing for the same funding dollars. I wish we look at censorship more collaboratively...We are now at a stage where we no longer have to scramble for funding, but unfortunately I don't think as a community we have that 'we are in this together' mindset." (P4)

Some providers highlighted that due to limited resources, they have had to degrade their services when user demand exceeded their capacity. P6 and P8, for example, shared situations where they had to throttle their traffic during recent surges in users, so that a larger number of users received some level of connectivity, albeit degraded.

The possibility of monetizing CT services through user payments or advertising has been considered by providers as a potential way to sustain their operations. Providers have considered accepting cryptocurrency as an alternative payment method or subsidizing free CT services with revenue from other sources (e.g., paid, western-focused VPNs). However, these efforts face complexities due to privacy and security concerns, given the elevated threat models of both providers and users, as well as the regions where these tools are most used.

> "It's difficult to monetize the service in a way that doesn't expose developers and providers to additional risk. With KYC (Kow Your Customer) and anti-money laundering / terrorism financing laws, it's hard to monetize without revealing our identities while also allowing common payment methods." (P7)

Usability U18 characterized the censorship in China as "*The Wall serves as a filter - anyone with enough technical knowledge can circumvent it.*" This observation aligned with the efforts of five providers, who highlighted being usable by people with varying technical skills as a key aspect of their tools. P4 explained their approach: "*as simple as possible, as our target users are not tech-savvy.*" P9 similarly remarked: "*We don't expect users to tweak it. We have to figure out how to make it work without telling users how they have to change things.*" Common usability efforts from providers include straightforward "one-click" UI designs and localized versions that offer various languages.

Most (n=13) surveyed users reported little to no usability issues, mainly with commercial VPNs or browser add-ons that require only "*average computer literacy*"(U7). This observation is consistent with prior studies [39]. The users appreciated the shift from complex interfaces to simpler, one-button connection options.

However, those who have used/attempted self-setup CTs (n=7) noted significant technical barriers. These solutions often require users to manage their own servers – a task that is already too complex for non-technical users. Additionally, most self-setup CTs are highly customizable, supporting various protocols and use cases, but this flexibility often demands deeper technical understanding and more manual configurations than "one-click plug-and-play".

> "All of them are total crap from the UI perspective. Nothing is explained. You choose between options gibberish1 and gibberish2 all the time. They made us all experienced users, even the ones who weren't tech savvy before." (U4)

A provider offering self-setup protocols echoed the confusion non-technical users face, particularly with the requirement of managing their own servers.

> "The fact that [our protocol] needs a server is a challenge. We try to make it easier by simplifying access keys and so on, but many users still just download the client app and are not sure what to do." (P6)

Finally, CT users also reported usability issues stemming from server-side security policies that discriminate against CT/VPN traffic. Common problems include applications detecting and blocking VPNs, increased encounters of CAPTCHAs, and local websites geoblocking foreign proxy IP addresses. These negative experiences align with findings from research on VPN adoption [57].

5.4 Trust and Risk Considerations

Next, we asked both providers and users about their perceptions of the risks involved in operating and using CTs, and the role of trust in this context. Both groups identified two primary types of risks – one related to the use of proxy or tunneling tools in general, and the dangers posed by authorities given that CT operation and usage is often illegal. These risks are interconnected and may exacerbate each other. For example, the potential consequences from CT usage heightens the threat model for users, which makes the security implications from proxy operator's possible misconduct even more critical.

Risk from Authorities Several participants highlighted an increased risk associated with operating, distributing, or sharing CTs, compared to simply using them. U18 commented "*The police don't care if it's just you. But if you're spreading it, then there's more likely to be legal issues*". For this reason, users mentioned that they only share access to their CT with close, trusted individuals. Providers echoed this observation, expressing their concerns for their in-situ distributors.

> "[CT] Distributors living in China or similar regions are under the jurisdiction of governments that apply censorship... There have been cases where they get felony for running anti-censorship services." (P7)

On the other hand, there's less clarity and agreement among participants regarding the consequences of just being a CT user. Participants from Russia indicated they don't perceive any legal issues with using CTs, provided that the tool is able to bypass the blocking; though, some highlighted the fragility of this status. "*I'm very afraid that a political decision to ban all and any VPNs can be taken.*" (U6). In China, while the use of CTs is technically illegal, participants noted that they never heard of anyone facing legal consequences merely for using circumventing solutions. "*I was using VPNs like everyone else*" (U14). Yet, participants also acknowledged the existence of an ambiguous "red line". For example, discussing CTs is perceived to be riskier than using them, and using CTs for political purposes, as opposed to leisure or entertainment, similarly carries its own set of risks.

Risk from Misbehaving Providers CT users, like users of other tunneling tools such as VPNs, are essentially transferring trust from their local network providers onto the CT providers, who are in a privileged position to collect and potentially profit off users' data. Participants voiced concerns about privacy risks from operators who might mishandle users' traffic. U13 shared a previous incident where "*some user data was leaked by one of the developers who was paid by [redacted]. I stopped using the service. They still were not transparent about what happened.*"

An even greater concern is the potential for misbehaving CT providers to collude with the authorities. Five surveyed users feared that CTs could be government-backed honeypots, or at least obligated by law to cooperate with the government's demands, such as sharing logs or filtering contents.

Trust and Mistrust These risks escalate the threat model for users, also emphasizing the importance of trust between CT users and providers. Providers we surveyed shared their various efforts to earn and maintain this trust, such as being more reliable in this volatile ecosystem:

> "Initially we assume there is no inherent trust. We gain trust primarily by working well."(P5) "...that the tool works reliably is the single most important factor to build trust."(P8)

In addition to providing reliable services, some providers aim to build trust through transparency about their operations. P10, for example, mentioned associating their service with their real names, offering a level of personal accountability:

> "I grew up in China and have friends there, so it's a decision I didn't take lightly. But I decided to not be anonymous precisely because people can look up where I got my education and what I do for work, and know I'm not a honeypot... Plus, if anything ever happens to me, someone would notice." (P10)

P9 elaborated on efforts to increase transparency such as having a clean background on the CT's ownership and building open-source software that allows independent audits:

> "In this space everything is trust. We are fully open-source and conduct 'no logs' audits every year. We say where we are based, and that we are a public organization with a clear and established background in this field... When we are blocked we also transparently communicate what is happening." (P9)

Providers also aim to build trust by exercising particular caution in their collection and handling of user data. For example, to minimize data collection, P5 claimed they "*don't see incoming IPs, only do a MaxMind lookup and then toss away. Don't gather any user info. Don't ask anything non-generic.*" For providers that accept payments, they implement mechanisms to separate CT usage records from payment records, as the latter often contains more identifiable information. These protective measures often exceed the typical safety protocols noted in studies of commercial VPNs [57].

Despite these efforts, there remains a widespread sense of mistrust between providers and users, a sentiment acknowledged by both sides (n=15U, n=8P). Many participants attributed this mistrust to the covert nature of censorship and the potential legal and personal risks involved. U14 shared the challenges in fostering a sense of community and trust:

> "It's good to have a community, but it doesn't exist because [CTs] are technically illegal in China, and there's so much distrust and snitching going on that unfortunately I just can't trust anyone." (U14)

Several providers noted that the frequent disruptions to CTs caused by censorship also impede the building of trust over time. P9 pointed out that the general lack of understanding among users about the technical aspects of CTs often leads to misattributing blocking-induced connectivity issues:

> "Users don't understand what a VPN, a protocol, or an IP is. Understanding connection errors and correctly attributing them is even harder. Often, users don't know what's happening and tend to blame you [CT providers] rather than government censors." (P9)

P7 and P10 mentioned that the trust relationship between users and providers, while initially founded on mutual goals of bypassing censorship, can be fragile under duress of legal and governmental pressure. For example, when confronted by the authorities, providers might shift their priority from providing access to self-preservation, a possibility that fuels users' cautious approach to trust.

> "I ask [other providers] why they require users to submit their IDs. They are not honeypots, but rather they keep this information so that if the government comes knocking, they have something to bribe - like saying 'Don't put me in jail, put these people in jail'." (P10)

The precarious legal standing of CTs, in contrast to other online services operating within regulated frameworks and

industry standards, leads to some dubious practices among providers. Examples include providers marketing their services with security claims that are impossible to verify, such as "no log policy" or "impossible to block", or operators profiting from spamming and advertising. One provider also discussed the differing notions of OSS among developers and raised doubts about the actual security assurances these open-source claims offer. These practices in the CT market also contribute to the overall lack of trust.

Access over Trust Despite the mistrust and significant risks associated with CT usage, these considerations surprisingly have limited influence on users' decisions to start using a CT. Many users adopt a pragmatic approach to using CTs, motivated not by trust in the CT's security or the operator's integrity, but by the sheer need to access censored resources.

For some users, this perspective reflects a resigned acceptance of the limited options available in a heavily censored environment, where the need to access information justifies using any available CT regardless of its trustworthiness:

> "I use whatever VPN that gets me connected. I don't know how it works, but since I had to use it, I had to trust it." (U16)

For others, indifference towards trust comes from a calculated assessment of risks; trust is considered irrelevant as long as their use of CTs does not involve high-stakes activities:

> "I don't trust the tool at all. For any activities beyond reading the prohibited sources I wouldn't use it. I would post something sensitive only outside the border. So for me it's enough if the tool just works." (U4)

Providers also recognize that users in the CT market often face the choice between using a potentially insecure tool or lacking access to censored contents:

> "Users tend to use any software that connects, even if it triggers antivirus alerts. They often face a choice between using this shady software to access the [uncensored] Internet or hardly having it at all. I can't say for everyone, but I'll sum up as: trust matters but not to a great extent." (P1)

Misconceptions When discussing the risks of CTs and the threat they can mitigate, there exists a disconnect between providers' priorities and users' expectations. CT providers, focusing on enabling access to content restricted by censorship, typically prioritize access above all other features.

> "I believe it is important to separate anonymity, privacy, and censorship circumvention, as they are quite different. Average users don't know the difference and just use the term 'VPN"'(P1) "We emphasize access over privacy-enhancing" (P4)

Yet, some users attribute additional security properties to CTs, such as online anonymity, privacy from local Internet providers, or security on unsecured networks. These expectations are more aligned with dedicated tools (e.g. Tor, default-gateway VPNs), rather than the objectives of standard CTs.

> "I look for anonymity...in the sense that I can easily disconnect myself. I don't want to be tracked down."(U22) "People use CT not just to unblock sources but to hide from their own Internet providers and police that they are reading [redacted]." (U4)

This gap in understanding can potentially put users at risk, since it may foster a false sense of security from tools primarily engineered for access.

6 Identified Future Priorities & Discussion

Our findings highlight multi-dimensional challenges that stakeholders in the CT ecosystem must navigate. These challenges are not limited to the technical aspect of circumvention (e.g., protocol obfuscation), but also cover areas such as service discovery, funding support, usability issues, and trust and risk considerations, each critically affecting the sustainability of the CT ecosystem. In the concluding part of our interviews with both providers and users, we shifted from the semi-structured interview protocols to more open-ended discussions, where we explicitly asked participants to identify the most pressing issues of the CT ecosystem and their views on future priorities for stakeholders. These dialogues were intentionally unstructured and often extended beyond the allocated time. In this section, we outline several themes that repeatedly surfaced throughout these discussions.

Bootstrapping Challenges The initial bootstrapping stage is a significant yet often overlooked challenge for users in censored regions. This stage involves making the first contact with a provider, acquiring client software and configurations, user authentication, *etc.* Most of these actions require a connection to the CT provider, which censors often obstruct. Yet, the CT itself cannot facilitate such connections until the bootstrapping steps are completed. For this, many systems, both in deployment and academic proposals, presuppose the existence of an "out-of-band" channel (e.g. [12, 19, 29, 36, 37, 47, 63, 68, 79]). This assumption not only complicates usability and wider adoption but also introduces potential security risks. As shown in this work, users might knowingly use less secure VPNs temporarily in order to bootstrap CTs, or they could have to install software from unverified sources if CTs are restricted on mainstream distribution channels like appstores.

Complicating the issue further, many bootstrapping steps need to be repeated following a server or key rotation (e.g. after blocking). One provider noted that requiring users to fetch updated IPs and keys, and then knowing how to apply the updates to their clients, is their main usability issue, as "*the more steps you have, the fewer people can do*" (P3). Developing secure and reliable methods for distributing CT software and

streamlining the bootstrapping and server rotation process remain a critical area for future research.

Outreach & Feedback Channels Establishing and maintaining resilient outreach and feedback channels is highlighted by both sides as a priority. Users acknowledge that service disruptions are often inevitable in the adversarial environment in which CTs operate. However, they stress the need for a reliable channel that remains accessible even during blocking incidents, allowing them to receive support and updates on the CT's status. For providers, maintaining a feedback loop with in-situ users is critical, especially during efforts to restore service after a blocking event, when immediate user feedback is essential for testing the effectiveness of any fixes. The absence of such feedback loops with in-situ users blocks iterative improvement and complicates the development cycles of CTs.

Providers highlight the importance of adapting outreach strategies to local norms and the value of establishing a local presence or partnering with local entities within censored regions to connect with users. These local partners, who are more familiar with the cultural and regulatory norms, can facilitate communication while also ensuring sensitivity to the users' environments and the ethical implications involved in engaging with users in these areas.

Flexible Funding CT providers often operate in a market characterized by volatile and unpredictable demands, particularly in the wake of major political or social events that trigger sudden surges in user numbers. For this, providers emphasize the need for two types of funding: long-term funding for sustainable development, research, and maintenance of their services; and short-term, emergency funding to quickly scale services in response to event-induced demand spikes. For the latter, initiatives like the OTF's Surge and Sustain Fund [6] aim to address these needs by helping to offset the marginal costs related to demand surges. Providers are calling for more accessible rapid-response funding opportunities with shorter application cycles and faster turnaround times to allow them to accommodate sudden influxes of users and maintain uninterrupted service during critical periods.

The fact that most funding comes from entities associated with government bodies restricts funding opportunities for grassroots CT providers operating within countries like Iran or Russia, where funding agencies like OTF cannot provide financial support due to trade restriction or export sanctions. Moreover, in regions like China, receiving funds from foreign governments, particularly the U.S., is often perceived as risky or unlawful, compelling local providers to distance themselves from such funding sources. Private grants or donations could serve as viable alternative funding avenues.

Academic Priorities vs. On-the-ground Needs The circumvention arms race demands continuous research and development efforts by CTs to keep up with evolving censorship techniques. However, providers noted a disconnect between the priorities of academic researchers and RFC/Internet standard designers, and the needs of CT users and developers in censored regions. Existing general-purpose protocol suites (e.g., OpenVPN), for example, were rarely designed with the censorship threat model in mind, and their architects often show little interest in engaging in the cat-and-mouse game [49]. Moreover, the localized nature of censorship practices places researchers based outside the censored regions at a disadvantage. As one provider puts it, it's "*like trying to solve a problem you don't experience or understand.*" (P4)

Academic research often values novelty over incremental improvements, prioritizing developing new concepts over improving the usability of existing tools. For example, recent studies on re-purposing voice chat or online games as circumvention transports, while academically appreciated, often fall short of translating into tangible, deployable solutions that address the simpler, practical needs of users facing censorship.

User Education Both providers and users identified inadequate user education as a significant barrier to CT adoption. This issue goes beyond basic usability or learning to use the tool; it's about understanding of what a CT is, how it works, the associated risks, and the specific threat models they address or fall short against. Multiple users shared their struggle in understanding how exactly CTs bypass censorship, which complicates their ability to make informed trust and risk assessments. Inadequate education also contributes to their stigmatization, often fueled by government propaganda linking CT use to cybercrime. Appropriate user education could help demystify CTs and encourage broader adoption. Moreover, providers highlighted a related concern of users prioritizing access and speed above security and privacy, which likely stems from the same gap in education. Better informing users about the exposure involved in using CTs and the risks from malpracticing providers could enable them to make educated decisions on whether to use CTs and which CT to choose. Yet, the question of *how* to safely and effectively engage users given the associated risks remains a challenge.

The importance of user education has been similarly noted by studies on the commercial VPN sector [57] and is echoed by similar initiatives from privacy-enhancing technologies (in more "open" countries). For example, Tor, which has long sought to dispel misconceptions and stigma around its use, provides educational resources that explain how it works and showcases its diverse variety of use cases by military, journalists, and "normal people" [10].

Collaboration & Community There are no simple solutions to many of the issues surfaced from our interviews. While generic recommendations such as increasing funding, communication, or expanding user education might appear as straightforward, the highly localized nature of censorship practices (and corresponding circumvention strategies) demands solutions tailored to specific regions. For example, our findings (§ 5) reveal that due to the different censorship land-

scapes in Russia and China, users in these two countries have different needs and priorities when it comes to circumvention.

A key aspect underlying many identified priorities is the need for providers and researchers to engage with local grassroots groups in censored regions for a better understanding of the specific censorship practices and user needs. Establishing effective communication with these groups, however, presents both technical and ethical complexities, especially in the presence of active adversaries. Some participants suggest that, where safe, in-person meetings could offer a more trusted space for stakeholders to share knowledge and experiences. Similarly, there's also a growing recognition among providers themselves of the need to foster collaboration and a sense of community, encouraging providers to view each other as allies rather than rivals competing for limited funding. A "we are in this together" mindset could lead to more efficient resource pooling, timely sharing of data and insights, and collective actions in response to censorship incidents, which would not only address immediate priorities but also facilitate the passing of knowledge and "lessons learned" across current and future generations of stakeholders in the CT ecosystem.

7 Conclusion

The escalation of censorship efforts by nation-state actors has fueled a surge in demand for circumvention tools across the world's most restricted networks. Yet, the ecosystem surrounding CTs remains largely opaque to researchers and regulators, due to its adversarial nature and the inherent risks faced by those directly involved. This exploratory study represents the first multi-perspective survey to shed light on the needs and challenges of both CT providers and users on the ground. We hope our study raises awareness and encourages further research, advocacy, and concerted efforts among stakeholders, academia, and funding bodies to improve the efficacy and sustainability of the CT ecosystem.

8 Acknowledgement

The authors would like to express their deepest gratitude to Jed Crandall and Armin Huremagic for their feedback, insightful discussions, and thorough review of this work. Their contributions have greatly improved the quality of this research. We also extend our thanks to Kyle Astroth for her assistance in conducting the study. Finally, the authors appreciate the constructive feedback provided by the anonymous reviewers. This material is based upon work supported by the National Science Foundation under Grant Numbers CNS-2237552 and CNS-2141512.

References

[1] Cyberoam firewall blocks meek by TLS signature — groups.google.com. https://groups.google.com/g/traffic-obf/c/BpFSCVgi5rs.

[2] dnstt; DoH- and DoT-capable DNS tunnel — bamsoftware.com. https://www.bamsoftware.com/software/dnstt/.

[3] Internet shutdowns in 2021 report: India is the world's largest offender. https://www.accessnow.org/internet-shutdowns-india-keepiton-2021/.

[4] Iran blocks social media, app stores and encrypted DNS amid Mahsa Amini protests — ooni.org. https://ooni.org/post/2022-iran-blocks-social-media-mahsa-amini-protests/.

[5] Missing Links: A comparison of search censorship in China - The Citizen Lab — citizenlab.ca. https://citizenlab.ca/2023/04/a-comparison-of-search-censorship-in-china/.

[6] OTF - Surge and Sustain Fund. https://www.opentech.fund/funds/surge-and-sustain-fund/.

[7] Shadowsocks | A fast tunnel proxy that helps you bypass firewalls. — shadowsocks.org. https://shadowsocks.org/.

[8] The President signed the law on sustainable Runet. https://d-russia.ru/prezident-podpisal-zakon-ob-ustojchivom-runete.html.

[9] Tor partially blocked in China | Tor Project — blog.torproject.org. https://blog.torproject.org/tor-partially-blocked-china/.

[10] Tor Project - Users of Tor. https://2019.www.torproject.org/about/torusers.html.en.

[11] VMess protocol | V2Fly.org — v2fly.org. https://www.v2fly.org/en_US/developer/protocols/vmess.html.

[12] Yawning Angel / obfs4 · GitLab — gitlab.com. https://gitlab.com/yawning/obfs4.

[13] Who is shutting down the internet in 2023? A mid-year update. https://www.accessnow.org/publication/internet-shutdowns-in-2023-mid-year-update/.

[14] Alice, Bob, Carol, J. Beznazwy, and A. Houmansadr. How China detects and blocks Shadowsocks. In *Internet Measurement Conference*. ACM, 2020.

[15] C. Anderson. Dimming the Internet: Detecting throttling as a mechanism of censorship in Iran. Technical report, University of Pennsylvania, 2013.

[16] S. Aryan, H. Aryan, and J. A. Halderman. Internet censorship in Iran: A first look. In *Free and Open Communications on the Internet*. USENIX, 2013.

[17] S. Aryan, H. Aryan, and J. A. Halderman. Internet censorship in iran: A first look. In *Free and Open Communications on the Internet*. USENIX, 2013.

[18] V. Braun and V. Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 2006.

[19] C. Brubaker, A. Houmansadr, and V. Shmatikov. CloudTransport: Using cloud storage for censorship-resistant networking. In *Privacy Enhancing Technologies Symposium*. Springer, 2014.

[20] A. Bryman. *Social research methods*. Oxford university press, 2016.

[21] X. Chen, J. Xie, Z. Wang, B. Shen, and Z. Zhou. How we express ourselves freely: Censorship, self-censorship, and anti-censorship on a chinese social media. In *International Conference on Information*, pages 93–108. Springer, 2023.

[22] J. Crandall, D. Zinn, M. Byrd, E. Barr, and R. East. Conceptdoppler: A weather tracker for internet censorship. pages 352–365, 01 2007.

[23] A. Dal and E. C. Nisbet. Walking through firewalls: Circumventing censorship of social media and online content in a networked authoritarian context. *Social Media+ Society*, 8(4):20563051221137738, 2022.

[24] K. P. Dyer, S. E. Coull, T. Ristenpart, and T. Shrimpton. Protocol misidentification made easy with Format-Transforming Encryption. In *Computer and Communications Security*. ACM, 2013.

[25] R. Ensafi, D. Fifield, P. Winter, N. Feamster, N. Weaver, and V. Paxson. Examining how the Great Firewall discovers hidden circumvention servers. In *Internet Measurement Conference*. ACM, 2015.

[26] R. Ensafi, P. Winter, A. Mueen, and J. Crandall. Analyzing the great firewall of china over space and time. *Proceedings on Privacy Enhancing Technologies*, 1, 04 2015.

[27] D. Fifield. *Threat modeling and circumvention of Internet censorship*. UC Berkeley, 2017.

[28] D. Fifield and M. G. Epner. Fingerprintability of webrtc, 2016.

[29] S. Frolov, J. Wampler, S. C. Tan, J. A. Halderman, N. Borisov, and E. Wustrow. Conjure: Summoning proxies from unused address space. In *Computer and Communications Security*. ACM, 2019.

[30] S. Frolov, J. Wampler, and E. Wustrow. Detecting Probe-resistant Proxies. In *Network and Distributed System Security*, 2020.

[31] S. Frolov and E. Wustrow. The Use of TLS in Censorship Circumvention. In *Network and Distributed System Security*. The Internet Society, 2019.

[32] G. Gebhart and T. Kohno. Internet censorship in thailand: User practices and potential threats. In *2017 IEEE European symposium on security and privacy (EuroS&P)*, pages 417–432. IEEE, 2017.

[33] GreatFire.org: We monitor and challenge Internet Censorship in China. https://zh.greatfire.org/.

[34] N. P. Hoang, A. A. Niaki, J. Dalek, J. Knockel, P. Lin, B. Marczak, M. Crete-Nishihata, P. Gill, and M. Polychronakis. How great is the Great Firewall? Measuring China's DNS censorship. In *USENIX Security Symposium*. USENIX, 2021.

[35] A. Houmansadr, C. Brubaker, and V. Shmatikov. The Parrot Is Dead: Observing Unobservable Network Communications. In *2013 IEEE S&P*.

[36] A. Houmansadr, T. Riedl, N. Borisov, and A. Singer. I want my voice to be heard: IP over voice-over-IP for unobservable censorship circumvention. In *Network and Distributed System Security*, 2013.

[37] J. Karlin, D. Ellard, A. W. Jackson, C. E. Jones, G. Lauer, D. P. Mankins, and W. T. Strayer. Decoy routing: Toward unblockable Internet communication. In *Free and Open Communications on the Internet*. USENIX, 2011.

[38] Y. Kou, Y. Kow, and X. Gui. Resisting the censorship infrastructure in china. 01 2017.

[39] Y. Kou, B. Semaan, and B. Nardi. A confucian look at internet censorship in china. In *Human-Computer Interaction-INTERACT 2017*. Springer, 2017.

[40] G. Kwak-Danciu. Vpn activism: Defending freedom and truth by circumventing internet censorship, Feb 2024.

[41] B. Marczak, N. Weaver, J. Dalek, R. Ensafi, D. Fifield, S. McKune, A. Rey, J. Scott-Railton, R. Deibert, and V. Paxson. An analysis of China's "Great Cannon". In *Free and Open Communications on the Internet*, Washington, D.C., Aug. 2015. USENIX.

[42] A. Master and C. Garman. A Worldwide View of Nation-state Internet Censorship. In *Free and Open Communications on the Internet*, 2023.

[43] N. McDonald, S. Schoenebeck, and A. Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice. *ACM on Human-Computer Interaction*, (CSCW), 2019.

[44] M. B. Miles, A. M. Huberman, J. Saldana, et al. Qualitative data analysis: A methods sourcebook. *Thousand Oaks, CA: Sage*, 2014.

[45] H. Mohajeri Moghaddam, B. Li, M. Derakhshani, and I. Goldberg. SkypeMorph: Protocol obfuscation for Tor bridges. In *Computer and Communications Security*. ACM, 2012.

[46] Y. Mou, K. Wu, and D. Atkin. Understanding the use of circumvention tools to bypass online censorship. *New Media & Society*, 18(5):837–856, 2016.

[47] M. Nasr, H. Zolfaghari, and A. Houmansadr. The waterfall of liberty: Decoy routing circumvention that resists routing attacks. In *Computer and Communications Security*. ACM, 2017.

[48] OknoDigital. Free and reliable vpn for those who care. https://okno.digital/.

[49] Thread: [openvpn-users] question about tls-crypt and port 443 firewall ducking. https://sourceforge.net/p/openvpn/mailman/message/35560747/.

[50] Outline VPN - Access to the free and open internet. https://getoutline.org/.

[51] P. Pearce, B. Jones, F. Li, R. Ensafi, N. Feamster, N. Weaver, and V. Paxson. Global measurement of DNS manipulation. In *USENIX Security Symposium*. USENIX, 2017.

[52] Proton VPN: Fast, private, and secure VPN service. https://protonvpn.com/.

[53] Psiphon | Uncensored Internet access for Windows and Mobile. https://psiphon.ca/.

[54] R. Rambert, Z. Weinberg, D. Barradas, and N. Christin. Chinese wall or Swiss cheese? keyword filtering in the Great Firewall of China. In *WWW*. ACM, 2021.

[55] R. Ramesh, R. S. Raman, M. Bernhard, V. Ongkowijaya, L. Evdokimov, A. Edmundson, S. Sprecher, M. Ikram, and R. Ensafi. Decentralized Control: A Case Study of Russia. In *Network and Distributed System Security*, 2020.

[56] R. Ramesh, R. S. Raman, A. Virkud, A. Dirksen, A. Huremagic, D. Fifield, D. Rodenburg, R. Hynes, D. Madory, and R. Ensafi. Network Responses to Russia's Invasion of Ukraine in 2022: A Cautionary Tale for Internet Freedom. In *USENIX Security Symposium*. USENIX, 2023.

[57] R. Ramesh, A. Vyas, and R. Ensafi. "All of them claim to be the best": Multi-perspective study of VPN users and VPN providers. In *USENIX Security Symposium*. USENIX, 2023.

[58] M. Roberts. *Censored: distraction and diversion inside China's Great Firewall*. Princeton University Press, 2018.

[59] Z. Rosson, F. Anthonio, C. T. Sage Cheng, and A. Skok. Internet shutdowns in 2022: the KeepItOn Report — accessnow.org. https://www.accessnow.org/internet-shutdowns-2022/.

[60] On taking measures regarding services to bypass restrictions on access to illegal content. https://rkn.gov.ru/news/rsoc/news73700.htm.

[61] On approval of the Rules for centralized management of a public communications network. http://publication.pravo.gov.ru/Document/View/0001202002170013.

[62] R. T. Service. Vpns are not a-ok: Turkmen internet users forced to swear on koran they won't use them, Aug 2021.

[63] P. K. Sharma, D. Gosain, H. Sagar, C. Kumar, A. Dogra, V. Naik, H. B. Acharya, and S. Chakravarty. SiegeBreaker: An SDN based practical decoy routing system. *Privacy Enhancing Technologies*, 2020, 2020.

[64] F. Shen and L. Tsui. Public opinion toward internet freedom in asia: A survey of internet users from 11 jurisdictions. *Berkman Center Research Publication*, (2016-8), 2016.

[65] G. Terry, N. Hayfield, V. Clarke, and V. Braun. Thematic analysis. *The SAGE handbook of qualitative research in psychology*, 2, 2017.

[66] M. C. Tschantz, S. Afroz, Anonymous, and V. Paxson. SoK: Towards Grounding Censorship Circumvention in Empiricism. In *2016 IEEE Symposium on Security and Privacy (SP)*.

[67] D. Wang and G. Mark. Internet censorship in china: Examining user awareness and attitudes. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 22(6):1–22, 2015.

[68] Q. Wang, X. Gong, G. T. K. Nguyen, A. Houmansadr, and N. Borisov. CensorSpoofer: Asymmetric communication using IP spoofing for censorship-resistant web browsing. In *Computer and Communications Security*. ACM, 2012.

[69] Z. Wang, Y. Cao, Z. Qian, C. Song, and S. V. Krishnamurthy. Your state is not mine: A closer look at evading stateful internet censorship. In *Internet Measurement Conference*, New York, NY, USA, 2017. Association for Computing Machinery.

[70] Z. Weinberg, J. Wang, V. Yegneswaran, L. Briesemeister, S. Cheung, F. Wang, and D. Boneh. StegoTorus: A camouflage proxy for the Tor anonymity system. In *Computer and Communications Security*. ACM, 2012.

[71] C. Winfrey. Growing with the People: Insights from Outline VPN Providers — Okthanks — okthanks.com. https://okthanks.com/blog/2024/4/9/growing-with-the-people, 2024.

[72] P. Winter and S. Lindskog. How the Great Firewall of China is blocking Tor. In *Free and Open Communications on the Internet*. USENIX, 2012.

[73] M. Wu, J. Sippe, D. Sivakumar, J. Burg, P. Anderson, X. Wang, K. Bock, A. Houmansadr, D. Levin, and E. Wustrow. How the great firewall of china detects and blocks fully encrypted traffic. In *USENIX Security Symposium*, 2023.

[74] X. Xu, Z. M. Mao, and J. A. Halderman. Internet censorship in china: Where does the filtering occur? In N. Spring and G. F. Riley, editors, *Passive and Active Measurement*, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[75] X. Xu, Z. M. Mao, and J. A. Halderman. Internet censorship in China: Where does the filtering occur? In *Passive and Active Measurement Conference*. Springer, 2011.

[76] D. Xue, M. Kallitsis, A. Houmansadr, and R. Ensafi. Fingerprinting Obfuscated Proxy Traffic with Encapsu-

lated TLS Handshakes. In *USENIX Security Symposium*, 2024.

[77] D. Xue, B. Mixon-Baca, ValdikSS, A. Ablove, B. Kujath, J. R. Crandall, and R. Ensafi. TSPU: Russia's decentralized censorship system. In *Internet Measurement Conference*. ACM, 2022.

[78] D. Xue, R. Ramesh, ValdikSS, L. Evdokimov, A. Viktorov, A. Jain, E. Wustrow, S. Basso, and R. Ensafi. Throttling Twitter: an emerging censorship technique in Russia. In *Internet Measurement Conference*. ACM, 2021.

[79] W. Zhou, A. Houmansadr, M. Caesar, and N. Borisov. SWEET: Serving the web by exploiting email tunnels. In *Hot Topics in Privacy Enhancing Technologies*. Springer, 2013.

[80] J. Zittrain and B. Edelman. Internet filtering in China. *IEEE Internet Computing*, 2003.

A Appendix

A.1 Provider Interview Protocol

Below are the questions which serve as a basis for our interviews with providers of circumvention tools, as discussed in §4.2.

Q1. What is your expertise around circumvention tools? What is your job? Are you a developer, distributor, or operator of a tool? *Self-describe your role in the Internet freedom community.*

Q2. What type of tools do you recommend to users? Here, users are persons with average computer skills who come to you for advice on using circumvention tools. *Here, users are persons with average computer skills who come to you for advice on using circumvention tools.*

Q3. If you develop your own tools or operate proxies that you provide access to others, what are the different ways you reach users experiencing censorship? What are usually the different channels used to share and tell others about circumvention tools?

Q4. Say a tool malfunctions/goes down in a particular region, what steps do you take to first understand the censor's actions and What steps do you take to debug it and fix it?

Q5. What are the different ways you gain trust with your community and what role does trust play in your community? *For example, does trust matter? Or users are generally OK with even "free VPNs"*

Q6. Following previous question, what are some of your red flags and concerns when it comes to circumvention tools? What would make you NOT want to use/recommend a particular tool?

Q7. What are some usability issues you have seen users struggle with?

Q8. In your words, what are the main problems circumvention tool developers and distributors face? What are the main issues in this ecosystem?

Q9. What types of questions would you ask users experiencing censorship to understand the main issues that users have?

Q10. Is there anything else you want to emphasize or add?

A.2 User Interview Protocol

Below are the questions which serve as a basis for our interviews with users of circumvention tools, as discussed in §4.2.

Q1. What comes to mind when you think about your experience with censorship?

Q2. Walk us through what the process of finding and using a circumvention tool looks like for you?

- Was it free or paid?
- What features made you want to use them?

Q3. What does your journey of using the tool look like? Similarly, do you only use it for a certain category of sites? *Is it turned on all the time on your computer? Or on the family computer etc...?*

Q4. At any point, did the tool become unavailable/unusable and when that happens what steps do you take to debug it and fix it?

Q5. Typically how do people in your circles find a CT? What are usually the different channels used? *Examples include sharing via encrypted messaging services, local methods such as USB sharing, etc...*

Q6. How much trust do you have in the developers of these CTs, what are some ways or signals you use to put trust in them?

Q7. What are some of your red flags and concerns? What would make you not want to use these CTs? *Examples include, worry about government honeypots, fake tools that want to scam, etc...*

Q8. Do you notice the Internet behaving differently near sensitive events? *How do you prepare for these events?*

Q9. Have you helped friends/family use CTs?

- What are the technical issues you have seen yourself or have seen friends and family struggle with?
- What are some usability issues you struggled with?
- How accessible are these tools to non-technical people?

Q10. Lets say we have direct connections to people that develop these tools, what are a few problems that you can enumerate and say, if we solved these problems, that would make it easier? Ideally what issues would you like to see solved? What issues make tools unusable for you?

Q11. How should operators of CT typically try to advertise their tool?

Q12. What types of questions would you ask users experiencing censorship to understand how these tools are used and identify the main issues users have?

Q13. Before we leave, can we get some demographic information – can you confirm for us your gender identities, and age range?

A.3 Consent Form

Consent Form. Below is the consent form shown to participants before the start of the interview. We receive verbal confirmation that they understand before proceeding with the questions, as discussed in §4.3.

- I, _____, voluntarily agree to participate in this research study.
- I understand that even if I agree to participate now, I can withdraw at any time or refuse to answer any question without any consequences of any kind.
- I understand that I can withdraw permission to use data from my interview within two weeks after the interview, in which case the material will be deleted.
- I have had the purpose and nature of the study explained to me in writing and I have had the opportunity to ask questions about the study.
- I understand that participation involves understanding and answering questions about my experience with internet censorship and circumvention tools.
- I understand that I will not benefit directly by participating in this research.
- I agree to note taking occurring during my interview.
- I understand that all information I provide for this study will be treated confidentially.
- I understand that insights gained from my interview may be quoted in a published research paper, conference presentations, and research reports.
- I understand that if I inform the researcher that myself or someone else is at risk of harm they may have to report this to the relevant authorities — they will discuss this with me first but may be required to report with or without my permission.
- I understand that under freedom of information legalization I am entitled to access the information I have provided at any time while it is in storage as specified above.
- I understand that I am free to contact any of the people involved in the research to seek further clarification and information.