UCSOS: Designing a Rapid Response System for Students at Risk

Rohit [Redacted]

Abstract

In recent times, the threat of sudden detainment and deportation has become a growing concern, especially among international students. The uncertainty and lack of recourse in such situations prompted us to explore how technology might support individuals at risk. We conducted interviews with three people who are actively involved in assisting vulnerable communities and gathered their perspectives on what would be most helpful in emergencies. This paper summarizes those discussions and presents a threat model that reflects the capabilities of a powerful state adversary. Based on this, we propose a design for a mobile application focused on ease of use, enabling victims to share critical personal information with emergency contacts and rapid response teams, so they can act on the victim's behalf after contact is cut off. For immediate support, the app would also allow users to place a call to a trusted hotline that can record the interaction with the adversary. To protect user privacy, all communication and data storage would be encrypted, and the app itself would be disguised to avoid drawing suspicion. While we do not implement a working prototype, we provide a detailed system design that outlines how such a solution could be developed in future work.

1 Introduction

Over 30 graduate students at UCSD and 1000s across the country have had their student visas revoked without explanation. [4] According to UCSD, the authorities have not provided any justification for these terminations. Focusing on the specific UCSD incident, this situation is especially concerning for us as graduate students, as it demonstrates how immigration status can be revoked without warning or recourse, leaving individuals in an uncertain and potentially dangerous position. In some cases, students have been detained without prior notice, with video evidence showing masked agents apprehending individuals and placing them in vehicles with little explanation or opportunity to respond. [2]

Beyond the initial shock of visa revocation, many affected students have faced further difficulties. Several were stopped at airports or ports of entry, questioned without legal representation, and compelled to surrender their personal devices. [2] These cases highlight not only the severity of the risk but also the limitations of individual preparation when faced with a sudden, state-level threat.

In response to these concerns, we sought to explore how technology could help support individuals in moments of sudden detainment. Rather than proposing a solution based solely on technical intuition, we began by conducting interviews with people actively involved in advocacy and response efforts. Their input shaped our understanding of the core needs in such scenarios. Based on these conversations, this paper is structured as follows: we first present a summary of the three interviews, followed by a threat model that captures the capabilities of the adversary. We then define the problem in more concrete terms, propose a detailed system design that reflects the requirements we gathered, and conclude with a discussion of future directions for this work.

2 Summary of Interviews

For a thorough requirements analysis, we conducted three interviews with people in different roles across the activism community. Below is a summary of each interview and the key findings that steer the project:

2.1 Professor Lilly Irani

Professor Lilly Irani is an Associate Professor of Communication & Science Studies at UC San Diego. She has a background in studying the effects of technology on culture and social dynamics, as well as advocating for social justice/worker's rights. [3]

We chose to interview her because of her extensive technological background intersecting with her experience advocating for social issues. She was able to offer useful insight from the perspective of an organizer, and someone in the community. Specifically, she advised that while the technological aspects of security and deniability are important, what matters even more is effective advocacy and outreach, ensuring that the tools and resources reach as many people as possible within the community.

1. **Outreach** - The most important thing, Professor Irani emphasized, is that people are educated about the challenges they might face. For example, many graduate students here may be focused solely on their studies, without having committed any serious offenses or concerns about being abruptly detained. For any app or system to be truly effective, individuals need to first understand the realities of their situation and how such tools could support them.

   Following that, it is crucial that people are aware of the rights they have in these high-risk circumstances, and have a plan for what they might do. Many would never anticipate finding themselves in such scenarios and, under stress, may not know how to respond. Professor Irani directed us to a valuable example, a toolkit distributed to UCSD faculty [1], which offers guidance on setting up emergency contacts, understanding one's rights, protecting oneself and others, securing digital devices, and developing safety contingency plans with trusted networks. She advised that something like this would be extremely valuable if it were commonly distributed/common knowledge.

2. **Support System** - She also advised that it is essential to have a dedicated, accessible support system for people at risk. Currently, lawyers are heavily overextended, and there is no large, official, or widely recognized community outreach group for those seeking help or wanting to assist. Therefore, establishing an outreach network that enables people to connect with one another is crucial. Importantly, the focus should be on creating something easy to find and use, rather than on building a system that is perfectly cryptographically secure. For instance, she recommended using WhatsApp or Messenger's secure chat features because these platforms are more widely available and familiar than alternatives like Signal.

   Additionally, community members must understand the importance of operating within their legal boundaries and recognize that certain actions could expose them to prosecution for obstruction. For example, explicitly stating that you are providing refuge for people engaged in illegal activity could be considered obstruction, whereas offering refuge to anyone in need is generally acceptable.

Essentially, rather than prioritizing a technological solution that is airtight from a cryptographic standpoint, she advised that for such a system to be truly useful, it is vital that people first understand their situation, know how to respond, and have a widely recognized, accessible way to contact others and share information. While the communication channels can incorporate cryptographic security, this should be secondary to ensuring the solution is user-friendly and approachable.

2.2 Professor Megan Ybarra

Professor Irani referred us to have a chat with Professor Ybarra, who is more involved in the activism community. Professor Ybarra is also an Associate Professor in the Department of Communication at UC San Diego and has been active in the activism community for the past five years. Initially working on such activities at the University of Washington, she has continued her work at UC San Diego, spreading the stories of detained individuals to a wider audience. [5]

Professor Megan Ybarra's work focuses on exposing and dismantling the criminalization-to-deportation pipeline, particularly through her engagement with the Northwest Detention Center (NWDC) in Tacoma, WA. She co-authored Unjust Enrichment, a zine documenting legal actions against GEO Group for exploiting detainee labor, and co-created "A Hunger Strikers Handbook" along with a short documentary highlighting the 2014 hunger strike at NWDC. Her research is grounded in long-term relationships with individuals impacted by immigrant detention and centers their resistance and calls for abolition. In addition to her scholarly and activist work, she has also helped coordinate bond funds for people who have been detained unlawfully. Despite having been arrested for her involvement in these abolitionist efforts, she continues to pursue this line of research with commitment and resilience. [5]

The interview with Professor Ybarra offered several key insights that helped shape our understanding of the problem space and finalize a core set of requirements.

Firstly, Professor Ybarra emphasized the importance of establishing a rapid response team i.e. individuals trained to act as intermediaries between victims and legal resources. These staff members would be responsible for quickly identifying legitimate cases, responding to emergency calls, and directing individuals to appropriate support networks. Crucially, she noted that these responders should ideally be people whose own residential status does not put them at immediate risk, enabling them to act decisively and without hesitation.

She also highlighted the need for pre-emptive safety planning. Victims of detention or deportation threats should prepare a compact, shareable packet of critical personal information ahead of time. In the event of an encounter with authorities, the recommendation is to limit verbal interaction to showing a "Know Your Rights" card (red card), with all additional information being shared later through secure, trusted channels; ideally via the rapid response team.

One of the more innovative and practical solutions Professor Ybarra described came from grassroots organizing work in cities like Seattle. To maintain discretion and privacy, some individuals have repurposed everyday tools, like hiking apps, to covertly share their location with trusted contacts and automatically send alerts when they fail to return. She stressed that any technological solution must prioritize data security and user privacy, in direct contrast to more openly accessible models discussed in previous interviews.

In terms of application features, Professor Ybarra was clear that the following two capabilities are essential. The first is the ability to place a direct call to the rapid response team, with the option to record the interaction for documentation. The second is a single-click "panic" function to wipe all sensitive data from a user's phone in case of detainment or phone confiscation.

She concluded by stressing the importance of institutional support, urging that every campus or community institution should have a dedicated hotline for these types of emergencies. She pointed to the UAW hotline [1] at UC San Diego as a functioning model already offering assistance in such cases.

2.3 Activism Community Member

The interviewee, a fourth-year university student, has been actively engaged in immigrant rights and activism for the past three years. Their involvement spans both campus initiatives and broader community-based efforts, including volunteer legal aid and participation in advocacy campaigns. Through this work, the interviewee has developed close relationships with individuals at risk of deportation or detention and often receives messages from community members who fear encounters with authorities. To retain privacy and upon the interviewee's request, their identity is kept anonymous.

People in the community face many serious concerns. The interviewee noted that the most common fears include being suddenly detained without warning, losing access to their phones and personal data, and being unable to contact a lawyer immediately after detention. One of the most painful concerns is family separation, especially in cases where children may be left without guardians. Many individuals also feel confused about their legal options. Most do not understand the process of filing a habeas corpus petition or do not know how to begin preparing for legal defense. In addition, there is widespread anxiety about digital surveillance. Some people are hesitant to use unfamiliar apps or tools because they fear their data will be tracked or misused.

Some members of the community take small steps to prepare for the possibility of detention. A few people carry printed Know Your Rights materials (red card) or store emergency contacts on their phones using codes. Others have tried to speak with nonprofit lawyers in advance, though this is not always possible. However, when individuals are confronted by immigration officers, they often do not know how to respond. The interviewee explained that most people react passively. Fear, language barriers, and lack of legal knowledge all contribute to this response. It is rare for individuals to assert their rights or ask to speak with a lawyer in the moment. After someone is detained, their family members usually reach out to local advocacy groups for support. These community-based responses are often helpful, but delays in connecting with legal aid can negatively impact the outcome of a case.

Legal representation is another major issue. Some individuals have informal connections to lawyers or legal clinics, but most do not have attorneys they can contact quickly. Nonprofit legal organizations and volunteer-based clinics are often overwhelmed and cannot take on every case. As a result, people rely heavily on informal networks within the community to find help. This process can be slow and uncertain, particularly in emergency situations.

There is some interest in using digital tools to improve emergency communication. The interviewee said that people would consider using an app for SOS alerts, but only if it met specific criteria. The interface would need to be extremely simple, ideally with a one-button function. It should send alerts directly to trusted personal contacts, not to centralized servers or unknown organizations. People are also interested in features that allow for encrypted communication and the ability to erase data quickly if needed. Apps that are already trusted by the community, like Signal, are more likely to be used. Any new tool would need to be endorsed by local groups that have built trust with immigrant communities.

Views on anonymity vary within the community. Some individuals want to remain anonymous because they are trying to protect themselves and their families. Others prefer to be visible in order to ensure they receive help quickly if they are detained. A flexible tool that allows users to adjust their privacy settings depending on their situation would likely be more effective. The interviewee emphasized that people's needs change depending on their level of risk.

In closing, the interviewee stressed that new tools and systems must be built with the understanding that the current legal and immigration system is often hostile to the people involved. There is a strong desire for a community-controlled network of legal support. While many recognize that habeas corpus petitions are an important legal tool, the process feels distant and confusing. People need more education about their rights, but they also need practical tools that help them act quickly. Features like pre-filled legal forms and secure document storage would be useful. The interviewee summarized the challenge by saying that in many cases, the community needs to be able to move faster than the system allows.

3 Threat Model

We model a powerful state-level adversary capable of initiating immediate and unannounced detainment of the victim. This scenario reflects the primary concern raised across all interviews, particularly by the Activism Community Member, who noted that even well-prepared individuals often fail to act consciously under panic. Once detained, the adversary is assumed to have full physical access to the victim's device and may employ any means to extract stored data, including leveraging device vulnerabilities or forcing unlocks. We place no restrictions on the adversary's capabilities post-detainment.

We assume the Rapid Response Team (RRT), legal aid networks, and emergency contacts configured by the victim are trusted entities. These actors are not modeled as malicious and are assumed to handle received information responsibly. Similarly, we assume that communication between the victim and these parties is not actively tampered with (e.g., no man-in-the-middle attacks), although it may be subject to passive monitoring or later access if the device or call records are compromised.

The emergency hotline connection is treated as a trusted endpoint, but subject to post-call surveillance or audio recording analysis once the device is seized. As a result, our design emphasizes ease of access and one-tap triggering, rather than long-term confidentiality of spoken communication.

Emergency contacts are assumed to be non-malicious, and the storage of their information within the application is not actively targeted. We do not address adversaries who may compromise contacts after the alert is sent, nor do we account for impersonation or insider threats within the contact network.

Other adversaries, including low-resource attackers, opportunistic threat actors, or local device theft without institutional backing, are excluded from our threat model. These simplifications reflect the focus of this work on scalable and realistic state-level threats and enable a more concise and actionable prototype design.

3.1 Problem Statement

With growing awareness of state-level detainment risks, many individuals, particularly international students, live with the fear of being suddenly detained without warning, losing access to their phones and data, and being denied contact with legal support. The Activism Community Member highlighted that unprepared individuals often have no understanding of their legal options, while even those who carry precautionary tools like "Know Your Rights" cards may find themselves unable to act when panic, fear, language barriers, or lack of legal knowledge set in.

To alleviate this situation, there is a need for a simple and accessible mobile application that directly addresses the needs expressed by those at risk. Such an application should focus on two primary functions: first, enabling the victim to quickly place a call to a trusted hotline that can assist with immediate concerns and potentially record the ongoing interaction in the presence of an adversary; and second, allowing the victim to disseminate critical personal information to preselected emergency contacts and rapid response teams (RRTs), so they can coordinate external support if the victim becomes unreachable.

To preserve the victim's privacy, the application should ensure that all communication is encrypted and sensitive data is stored securely on the device. It should also include a simple mechanism to quickly erase this data in case of detainment. The app's appearance may need to be disguised to avoid attracting suspicion during device checks. Given the concern around digital surveillance and the reluctance to use unfamiliar apps, user adoption would likely depend on proper training and endorsement from trusted community networks.

Privacy for RRT members must also be considered. The application should support anonymized communication channels, with individual identities only revealed when out-of-band communication takes place. Additionally, the app should offer a built-in safety toolkit—a guided checklist that helps users prepare for emergencies by understanding their rights, securing their devices, and setting up contingency plans.

A key assumption here is the existence of a localized and trusted hotline and RRT. While our university setting provides a working example of such a support system, scaling this solution beyond a prototype would require building similarly trained networks—what Professor Ybarra described as individuals who are not at immediate risk and can act calmly and decisively in high-pressure situations.

4 System Design

The system is designed as a mobile application, prioritizing usability, speed, and privacy for users facing sudden state-level detainment risks. The architecture reflects three guiding principles: minimal user interaction in emergencies, secure communication and data handling, and community-driven adoption. We also present a set of wireframes in Figures 1 and 2 that demonstrate how the application interface can be structured around these core features.

4.1 Core Features

4.1.1 Rapid Response Hotline

The main interface provides a prominent "Call Hotline" button, enabling the user to contact a pre-configured Rapid Response Team (RRT) with a single tap. The call is routed through the device's telephony stack to avoid raising suspicion. Where permitted by local law, the call may be automatically recorded and stored in a secure, encrypted partition. The application also displays a "Know Your Rights" statement on screen during the call, offering users a script to assert their rights under duress.

4.1.2 SOS Alert and Data Broadcast

A separate "SOS" button initiates a one-tap broadcast to selected emergency contacts and RRT members. This broadcast contains critical information such as full legal name, birthdate, alien number, country of origin, last known location, and/or any pre-entered personal or legal details necessary to initiate external advocacy or legal action. Where possible, the alert is sent using end-to-end encrypted channels (e.g., Signal protocol or secure messaging APIs) if the recipient uses the same application or has public keys available—for example, trusted RRT members. For broader dissemination to emergency contacts who may not have compatible tools or pre-shared keys, the message is sent in plaintext, prioritizing reach and accessibility in time-sensitive scenarios. To accommodate users' varying privacy needs, the app allows granular selection of which data is included in the alert. To prevent an accidental SOS being sent, we require the user to swipe up on the button and hold for 5 seconds (user configurable length).

4.1.3 Emergency Data Wipe

Recognizing that physical device compromise is likely, the app supports a panic-trigger function. Triggered via a hardware button sequence or on-screen action, this securely erases all encrypted sensitive local data (including app history, contacts, and recordings) by overwriting and removing cryptographic keys from the device storage. This feature aims to mitigate data extraction by adversaries post-detainment.

4.1.4 Disguised Interface and Access

To prevent pre-emptive suspicion, the application may operate in a "camouflage" mode, adopting the appearance of an innocuous utility (such as a calculator or notes app). Access to the actual emergency features requires entering a pre-set PIN or gesture, offering plausible deniability.

4.1.5 Safety Toolkit and Preparation Guide

The app includes a built-in "Safety Toolkit," featuring:

- A customizable checklist for preparing legal documents and emergency contacts.
- Digital versions of "Know Your Rights" materials, available offline and in multiple languages.
- Guided steps for setting up contingency plans, inspired by UCSD's faculty toolkit and community best practices.

This component is accessible in non-emergency contexts and is designed to foster education and proactive planning.

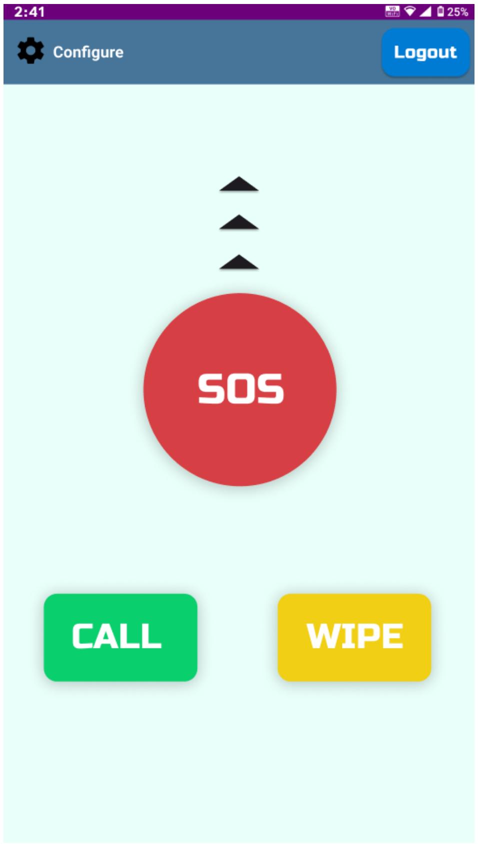

Figure 1: Users should be able to easily send distress messages, as well as call a hotline number and wipe relevant data.

4.2 Security and Privacy Architecture

4.2.1 Data Storage and Encryption

All sensitive data such as contacts, legal documents, user information, and recordings, are encrypted at rest using strong device-based cryptography (e.g., AES-GCM with keys tied to secure hardware modules when available). No data is stored externally or in the cloud by default, minimizing exposure in case of server compromise.

4.2.2 End-to-End Encrypted Communications

For alert broadcasts and message delivery, the app leverages proven secure messaging frameworks. If users already have trusted apps like Signal or WhatsApp installed, integration is offered to maximize adoption and minimize friction. Direct app-to-app communication is implemented only where trusted local infrastructure (e.g., RRT-run servers) can be verified.

4.2.3 Decentralized Trust Model

The design deliberately avoids centralized backends wherever possible. Instead, trusted contact lists are maintained on-device, and all communications are peer-to-peer or through established, community-vetted services. No identifying user data is shared outside the emergency context.

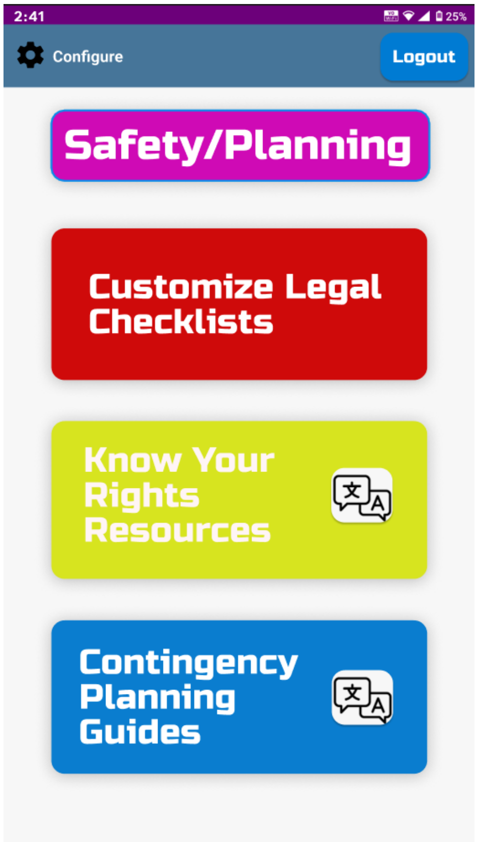
2:41
25%
Configure
Logout
Safety/Planning
Customize Legal Checklists
Know Your Rights Resources
Contingency Planning Guides

Figure 2: Users should be able to create legal checklists, and access resources on their rights/contingency planning, in the language of their choice.

4.3 User Experience and Adoption

4.3.1 Community-Centric Onboarding

In recognition of distrust toward unfamiliar digital tools, onboarding is conducted in partnership with community organizations. The application is distributed directly by trusted groups, and setup is guided via workshops, with privacy and risk explained in users' native languages.

4.3.2 Accessibility and Usability

Interfaces are simplified for rapid use under stress, with visual cues and large buttons. The "panic" and "SOS" actions require minimal interaction, and the app is designed to be usable for individuals with limited technical proficiency or language barriers.

4.3.3 Flexible Privacy Controls

Users can configure the level of anonymity for SOS alerts, choosing to include or exclude identifying information based on their perceived risk at the time of setup. Emergency contacts and RRTs can also interact via anonymized messaging within the app, only revealing full details in out-of-band channels as required.

5 Conclusion and Future Work

Our interviews revealed three key challenges: a general lack of awareness among students about the risks they face, limited tools or knowledge to advocate for themselves, and the difficulty of taking action under stress in real-time situations. These insights shaped our goal: to design a system that offers a quick, secure, and non-incriminating way to reach trusted contacts, while prioritizing usability and community familiarity.

While no technical solution can guarantee protection against a determined adversary with physical access to a device, our proposed design focuses on minimizing harm and enabling rapid support. Its success relies not only on the technical components but also on user preparation and strong, localized support networks. Continuous engagement with affected communities will be essential to ensure the system remains practical and trustworthy.

Although our current design is tailored to the university setting, the architecture is possible to scale. Future enhancements could include integration with legal aid tools, secure identity storage, or automated legal response mechanisms. Its modular structure allows adaptation to different legal and threat environments, making it a flexible foundation for broader use.

References

[1] COMMUNITY, U. Unofficial safety planning for ucsd community members. https://docs.proton.me/doc?mode=open-url&token=MEKCP87C5G&linkId=ZjZom_RryHJr1uzs6olGiEwbehjXLe2pKmKUC2l0SQJI1Lx7DlefHwX874_R2VfI0KO3_tLIQnDTbZXc1S9b8g%3D%3D#gdEtdlR3NJFZ, Apr 2025.

[2] DRENON, B. Why has trump revoked hundreds of international student visas? https://www.bbc.com/news/articles/cg411rrnkkko, Apr 2025.

[3] IRANI, L. Bio & cv. https://quote.ucsd.edu/lirani/photos-and-bio/.

[4] SMITH, D. Visas revoked from few dozen more uc san diego students, university says. https://www.nbcsandiego.com/news/local/uc-san-diego-student-visas-revoked/3806855/, Apr 2025.

[5] YBARRA, M. Meganybarra. https://www.meganybarra.com/.