Risk, Technology, and Resistance: The Hong Kong Diaspora Amid Transnational Repression

NOAH KEI, University of Toronto, Canada
ASHIQUE ALI THUPPILIKKAT, University of Toronto, Canada
HIU-FUNG CHUNG, University of Toronto, Canada
PRIYANK CHANDRA, University of Toronto, Canada

Diasporic Hong Kong communities are increasingly shaped by transnational repression, which is amplified through the sociotechnical systems within which they are embedded. In this context, risk is not merely a condition to be endured but a subjective, relational, and sociotechnical construct that modulates everyday social life and political organizing. Drawing on 11 semi-structured interviews with diasporic organizers in North America, we identify five interrelated forms of perceived risk — reputational harm, "Sam Tau" (滲透), infiltration, state surveillance, and non-state surveillance. These risks reveal how collective vulnerability emerges through both explicit repression and ambient uncertainty. In response, actors engage in boundary work — through gatekeeping, selective participation, and socio-technical vetting practices — to construct digital enclaves, maintain cohesion, and cultivate a risk-aware Hong Kong identity. This paper contributes to CSCW by extending existing scholarship on diasporic social movements, community moderation, and boundary maintenance, offering insights into how sociotechnical infrastructures are leveraged, and must be reimagined, for organizing under conditions of transnational repression.

CCS Concepts: • **Human-centered computing** → **Collaborative and social computing**.

Additional Key Words and Phrases: Digital Diaspora, Transnational Repression, Anti-regime Social Movement, Risk, Risk Mitigation, Vetting, Gatekeeping, Boundary Work, Trust, Informality, Digital Safety

1 Introduction

In the wake of the 2019–2020 anti-extradition protests (AEP) in Hong Kong, a new wave of politically active diaspora has emerged. These communities have been shaped not only by the urgency of exile in an increasingly autocratizing society [63], but also by the dual imperatives of sustaining political momentum and safeguarding both personal and collective security in host countries. Historically, Hong Kong has been characterized by scholars as a city of migration and a "refugee society", shaped by successive waves of displacement. However, the post-AEP diaspora marks a critical departure from these earlier migrations. This new formation is distinguished by its communicative infrastructure and transnational connectivity, afforded by a complex digital ecology in which the strategic (non-)use of certain social media and digital platforms becomes a necessity. Amid

Authors' Contact Information: Noah Kei, noah.kei@mail.utoronto.ca, University of Toronto, Toronto, Ontario, Canada; Ashique Ali Thuppilikkat, ashique.thuppilikkat@mail.utoronto.ca, University of Toronto, Toronto, Ontario, Canada; Hiu-Fung Chung, hiufung.chung@mail.utoronto.ca, University of Toronto, Toronto, Ontario, Canada; Priyank Chandra, priyank.chandra@utoronto.ca, University of Toronto, Toronto, Ontario, Canada.

increasing concerns over transnational repression through digital surveillance, legal instruments, and informal networks, diasporic organizers find themselves navigating a risky sociotechnical environment. In this context, risk is not merely a fixed or external condition to be endured but a dynamic, contested construct that structures diasporic life across social, cultural, and political dimensions.

CSCW and HCI scholarship has increasingly examined how diasporic communities use digital technologies to maintain cultural ties, mobilize dissent, and construct political identities across borders [7, 104]. From blogs to encrypted messaging platforms, these infrastructures support transnational activism while simultaneously exposing communities to new vulnerabilities. Recent work has shown how digital systems have become entangled with mechanisms of transnational repression through, for instance, cyberattacks, and proxy threats, posing significant risks to activists and organizers [3, 26, 42, 70, 73, 93, 96]. Building on this body of research, our study foregrounds risk not as a fixed or objective condition, but as a subjective, relational, and sociotechnical construct shaped by diasporic actors' perceptions and lived experiences.

We situate our analysis within CSCW scholarship on social computing under repression [39, 44, 53, 54], examining how diasporic organizers assess, negotiate, and respond to risk through boundary work, gatekeeping, vetting, and selective participation practices that are intended to preserve community safety, cohesion, and organizing. In doing so, we contribute to ongoing conversations in HCI and CSCW about how socio-technical systems both enable and constrain political participation under authoritarian pressure. Our work addresses a gap in the literature by analysing how risk negotiation and vetting practices operate in informal, hybrid digital spaces, with implications for platform design, trust-building, and solidarity in transnational diasporic communities.

Specifically, our paper responds to the following research questions:

(1) How do Hong Kong diasporic organizers in North America perceive and navigate risk in the face of transnational repression, and how is this shaped by their sociopolitical and sociotechnical contexts?
(2) How do sociotechnical practices mediate risk mitigation and sustain diasporic organizing efforts?

Drawing on 11 interviews with diasporic organizers, our findings suggest that risks shape collective identity, community, and technology practice. We identify recurring forms of perceived risk that reflect how risk is experienced not only as external coercion but as a relational uncertainty embedded in everyday life. These risks are shaped by prior experiences of repression, sustained through sociotechnical infrastructures, and modulated by existing platform affordances. We then explore how technologies mediate perceptions of risk and identity, showing how diasporic affiliations are curated, vetted, and maintained through digital platforms that simultaneously enable solidarity and produce new vulnerabilities. Participants respond to these conditions through adaptive sociotechnical practices of risk mitigation and boundary maintenance that function less as absolute protections but rather as ongoing calibrations of trust, visibility, and risk.

Our paper makes three contributions to CSCW, HCI, and social computing scholarship. First, we theorize how risk — as a socially situated and relational condition — is central to the construction of the diasporic identity in the face of transnational repression, which unfolds through authoritarian surveillant assemblages, wherein the state is one vector among many. Second, we challenge assumptions around transparency, openness, and inclusion, showing how these values must be reconsidered when visibility itself can constitute risk, and exclusion becomes a necessary condition for safety and social cohesion. Third, through exploring how diasporic organizers calibrate trust,

mitigate risk, and sustain organizing, we offer implications for the design of technologies that better support transnational diasporic organizing in the face of rising global repression.

2 Related Work

CSCW and HCI literature highlight how diasporas — though heterogeneous — maintain enduring emotional, cultural, and historical ties to their origin-homelands across generations, with these connections often acquiring heightened political significance in transnational social movements and conflict contexts [7, 10, 103]. Digital technologies — from blogs and social media platforms to encrypted messaging — have empowered these communities to construct identities, mobilize dissent, and amplify visibility [6, 7, 16, 30, 80]. Yet these same infrastructures also expose communities to new vulnerabilities, enabling extraterritorial authoritarian control [26, 93] and transnational repression—defined by practices such as digital surveillance, cyberattacks, physical violence, and harassment to silence dissent [3, 26, 42, 73, 96].

Recent scholarship identifies two dominant approaches to understanding contemporary transnational repression [100]. The first, the state-institutional model, focuses on formal mechanisms such as legal coercion [48] and media manipulation [72] through which regimes project authoritarian power abroad. The second, a relational approach, shifts attention to non-state actors within global migrant networks, which include nationalist diasporic groups that actively align with their origin-homeland regimes, participating in the suppression of dissident voices within diasporic spaces [100]. Studies also reveal informal tactics like proxy punishment: targeting activists' families in their home countries to suppress dissent overseas [74, 84].

Building on this body of work, this research tentatively categorizes the risks associated with transnational repression along two analytical dimensions: (1) the mode of technological (non-)use (e.g., digital surveillance vs. physical harassment) and (2) the degree of actor informality (e.g., formal state institutions vs. informal networked actors).

2.1 Navigating Risk in Anti-Regime Social Movements

Scholars analysing authoritarian contexts have identified the concept of an authoritarian surveillant assemblage — a dynamic network of interconnected surveillance systems that continuously expand in scope, forge new linkages, and integrate diverse actors [95]. This assemblage[1] combines synoptic media surveillance (which includes top-down state monitoring) with informant-collaborator systems (participatory repression), enabling regimes to exert pervasive social control [95]. For anti-regime social movements — including those operating from diasporic contexts — such configurations pose significant risks, as states deploy paid informants or security agents to infiltrate and disrupt movements from within, undermining their network relations [78].

Critically, the notion of risk in these contexts cannot be reduced to objective probabilities or narrowly framed threat models. Following Douglas and Wildavsky's [31] conceptualization of risk as culturally constructed and Slovic's [86] attention to the affective and cognitive dimensions of risk perception, we approach risk as a subjective and situated assessment of potential harm, characterized by uncertainty, and embedded in particular social, political, and historical contexts. Risk, in this sense, is not merely a precondition for decision-making but a socially distributed phenomenon that reflects individuals'/communities' subjective perceptions of potential harm and uncertainty, shaping their agentic decision-making, responses, predictions, and actions as they navigate contingencies or uncertain states of affairs [14, 17]. Anthony Giddens observes that risk,

---

[1]Assemblage configurations are never fixed, linear, or uniform; rather, they are constantly evolving through dynamic processes of adaptation and transformation, and their significance needs to be understood through how components interact rather than through any inherent qualities.

while often framed negatively as the anticipation of adverse outcomes, simultaneously enables positive action, serving as the calculative basis for action in the face of uncertainty [40]. Whether risk manifests as visceral perceptions of imminent threat or as calculated assessments grounded in logic and deliberation, both are responses to uncertainty [87].

For participants in anti-regime social movements, risk also manifests through the potential erosion of inclusive sociability — conditions where coercive and repressive constraints, institutional control, systemic exclusion, and oppression encounter individual and collective expression and spaces of engagement. Importantly, risk extends beyond mere security and safety concerns; it is fundamentally tied to responsibility [40] — the necessity of making consequential choices where outcomes are knowable yet uncertain. As sociocultural theories emphasize, the lived experience of risk — how it is dynamically understood, embodied, and negotiated within specific social contexts — also functions as a practice of boundary-making, one that simultaneously defines collective identities (Self/Other) and structures lived experiences of vulnerability [66].

To navigate these conditions, anti-regime social movements engage in boundary work: strict membership vetting, gatekeeping access and participation, cautious fundraising practices, and selective aid acceptance are employed to prevent external interference and internal fragmentation [22, 78]. While critical for preventing violence and ensuring movements' goal alignment [83], such practices can conflict at times with movements' collaborative and nonviolent ethos [78]. Furthermore, diasporic social movement participants also rely on forming transnational counter-publics, invisible networked publics, and counter-public enclaves in social media and online spaces to avoid state repression [7, 20, 58]. These strategies reflect more than just security measures; they shape political messaging, movement goals, and collective identity. Our work aims to provide CSCW, HCI, and social movement scholars with insights into the concrete modalities of boundary work, both around and beyond technology use.

2.2 Risk Mitigation, Boundary Work, and Social Computing for Anti-regime Diasporic Social Movements

While communication technologies like WhatsApp and Facebook serve as vital conduits of cultural, political, and epistemic knowledge for diasporas by connecting them to knowledge bearers and transnational networks [8], their usage involves careful risk assessment regarding personal safety and transnational repression — particularly for those engaged in politically sensitive contexts or social movements. Diaspora members — especially those fleeing persecution — recognize risks posed by both state and non-state actors and adopt various mitigation strategies, including anonymity maintenance, altered communication and phone usage patterns, disguised political messaging, and complete phone avoidance, to ensure personal safety [82, 105].

With respect to technology use, although diaspora members engage in sociotechnical adaptation — leveraging technologies and networks across host and origin-homelands to navigate new environments [50] — they often retain technology and platform dependencies rooted in origin-homeland. For instance, WeChat — which became 'infrastructural' for the Chinese diaspora in the United States — served purposes beyond communication, including fintech, business operations, and client management [104]. Furthermore, studies show that when risks associated with technology use are uncertain or ambiguous, trust in platforms often overrides potential concerns [43, 69, 99]. For instance, the reliance on Telegram as a protest tool in the 2020 Belarusian protests, even by the diaspora, demonstrates this dynamic—where perceived platform credibility outweighed risk assessments [99]. For social movement organizers and participants operating under risk, the CSCW community has also often emphasised social computing systems that prioritize designs to protect

them from repression and surveillance, including robust end-to-end encryption in messaging platforms to ensure secure communication [38]. At the same time, awareness and perceptions of risks could also potentially deter participation by vulnerable communities in social movements [101].

CSCW literature also warn of boundary turbulence—violations where a user's contacts become threat vectors through either careless or malicious disclosures of information, as they navigate networked community settings [43]. To minimise risk in such contexts, various organizational settings adopt vetting, a sociotechnical process, reflecting methods like background checks and surveillance in online and offline contexts [56, 67, 71]. While traditionally a precaution against risks stemming from deception, spies, and reputation damage, vetting has been explored through perspectives of state security and counter intelligence [71], business brand management and affairs in the economy and electoral politics [11, 32, 67, 68, 77], and coordination work in crisis informatics [25]. In most organizational settings, vetting typically occurs before recruitment or following training [49]. Similar practices are also deployed by substate actors [98], insurgent groups, rebels, and sub-nationalist movements (even operating from diasporic settings), for membership in communities formed on social media platforms such as Facebook and Telegram [27]. Vetting serves as a critical mechanism for network gatekeeping in digital safe spaces, exemplified by practices in women-only Facebook groups [5], review of applicants' social media histories [11, 32], and multi-stage screening processes involving nomination, voting, and in-person verification [36]. However, these established methods face significant challenges with anonymous newcomers [55] with unclear digital traces. While CSCW research has examined vetting through state security frameworks, little is known about how such practices are negotiated in informal spaces, hybrid contexts blending formal and informal logics, or social movements. Our study addresses this gap by investigating vetting practices, as part of boundary work, in diaspora-led social movements — spaces that uniquely navigate, negotiate, and permeate formal-informal boundaries.

Existing studies have also examined the boundaries of "privacy and publicness" [57] in information disclosure practices and community building during everyday online participation as well. This work has identified various tactics, including audience-specific information disclosure, pre-emptive content filtering, collaborative curation, and post-hoc content deletion [2, 9, 57]. Some manage boundaries through either a single account with granular privacy controls (e.g., restricting content to specific connections), or through multiple profiles enabling pseudonymity, separation, and practical obscurity [88, 89]. Notably, these studies have not investigated boundary regulation practices among diasporas navigating transnational repression—contexts entailing distinct and heightened risks. Our paper addresses this gap by contributing new insights to CSCW on how diasporas navigating transnational repression employ collaborative risk management strategies to sustain community building and online participation. Furthermore, our enquiry is informed by Palen and Dourish's [79] argument that people are not merely individuals but also members of broader social groups. Building on this, we assess how diasporas navigate risk assessments (which influence their boundary work) under conditions of transnational repression.

3 Data, Methods, and Limitations

Our data collection began in June 2024, five years after the onset of the 2019–2020 anti-extradition protests in Hong Kong and in the final stages of many countries' special migration and permanent residence pathways for Hong Kong residents. This period marked a moment of both political urgency and migratory transition. Throughout the research process, we centred participants' needs for privacy and safety. The first author, a long-standing member of the diasporic Hong Konger community, advised the research team on ethical considerations and sensitive points of inquiry. This included avoiding questions that might inadvertently provoke politically charged disclosures or psychological distress.

The research problem and initial research questions focused on collective identity, the processes of mobilization and organization, and the use of technologies before and after joining the diasporic community. However, participant narratives highlighted issues of surveillance, transnational repression, and risk management. Our final semi-structured interview protocol was organized into four categories: (1) Hong Konger identity; (2) perceptions of safety and risk; (3) experiences in the diaspora; and (4) the role of technology. The study received ethics approval from the authors' institutional review board.

3.1 Participants and Recruitment

We adopted a multi-faceted, purposive sampling strategy to recruit participants, with a focus on diasporic organizers. The first author, who was based in Hong Kong and witnessed the changing dynamics there since the handover to China in 1997, maintained strong ties with diasporic networks and initiated contact via discreet outreach to potential participants. We also distributed cold-call invitations through email to Hong Kong-related diasporic organizations across North America. Snowball sampling was subsequently used to extend our recruitment to include individuals with diverse positionalities within diasporic organizing, including gender, generation, organizational affiliation, and political engagement. All participants had attained or were pursuing tertiary education. Participants' ages ranged from 18 to 70, and their time in the diaspora spanned from under one year to over three decades. Our final sample included individuals affiliated with both formal and informal community spaces, such as religious groups, professional associations, student collectives, and independent cultural networks, with organization size ranging from 50 to over 20,000. Table 1 summarizes participant demographics and affiliations, with their specific locations withheld for security reasons.

Outreach to risk-aware diasporic organizers for research interviews was challenging due to the protective nature of digital enclaves. However, we estimate this sample size's accumulated sphere of influence to cover over 100,000 diasporic actors, a substantial and analytically meaningful portion of the broader diasporic Hong Kong communities and sufficient to initiate important discussion amidst rising global repression. More importantly, this sample size is methodologically appropriate for this qualitative design [46], in which contextual data were generated through in-depth interviews. These data enable interpretation of the lived experiences, risk negotiations, and organizational practices of diasporic actors embedded in socio-technical systems. Rooted in an interpretive qualitative tradition, this study does not aim for statistical generalization but instead seeks *analytical generalization,* offering conceptual insights transferable to other contexts of transnational repression and digital diaspora.

3.2 Data Collection and Analysis

We conducted semi-structured interviews with 11 diasporic organizers in Cantonese, the native language of Hong Kong, using Jitsi Meet — a free and open-source multiplatform voice (VoIP), video-conferencing, and instant messaging application — to protect participants' privacy. Each interview was audio recorded with verbal consent, with each participant receiving a $25 CAD honorarium. To safeguard anonymity and minimize exposure to risk, we deliberately avoided collecting legal or immigration status. Interviews were conducted by two native Cantonese-speaking researchers. All recordings were first transcribed in Cantonese by the first author and then translated into English to facilitate collaborative analysis with non-Cantonese-speaking members of the research team.

Although the first and third authors supported the rest of the team in understanding Hong Kong-style Cantonese phrases, the meanings were often difficult to translate into English. We recognise that we could potentially miss specific nuances and meanings; hence, the first author

conducted open coding, followed by iterative thematic coding in Cantonese, in consultation with the rest of the research team. Difficult-to-translate phrases were discussed collaboratively.

We conducted a reflexive thematic analysis [15] that proceeded in four stages: (1) familiarization with transcripts, alongside initial debriefing and memoing sessions, (2) development of initial codes by the first author, (3) iterative coding of transcripts through team discussions, and (4) constructing and reviewing candidate themes through recursive engagement with coded data. The final list of codes developed to support reflexive engagement contained 145 codes organized across 8 categories. The research team maintained analytic memos and decision notes to document the process, along with thematic maps to illustrate the relationships between the codes, themes, and sub-themes. Researchers met regularly to collectively define the themes and sub-themes, with the first and third authors verifying that the original Cantonese meanings were preserved. Example themes included risk as an organizing logic, selective visibility and identity management, organizing under surveillance, gatekeeping and vetting practices, scalability in diasporic organizing, among others.

Table 1. Summary of Participant Demographics and Affiliation

Participant	Age range	Gender	Residence	Type of organizers
S01	20 - 30	M	Canada	Cultural and Recreational Organizing
S02	40 - 50	M	Canada	Professional and Economic Organizing
S03	40 - 50	M	Canada	Religious and Community-based Organizing
S04	50 - 60	M	USA	Community-based Organizing
S05	60 - 70	M	Canada	Political and Economic Organizing
S06	20 - 30	F	Canada	Alumni and Educational Network Organizing
S07	50 - 60	M	USA	Professional and Youth Organizing
S08	20 - 30	F	Canada	Student Organizing
S09	20 - 30	F	Canada	Student Organizing
S10	18 - 20	F	Canada	Student Organizing
S11	30 - 40	M	Canada	Political and Cultural Organizing

4 Background

4.1 Hong Kong as a City of Migration

Hong Kong has been profoundly shaped by successive waves of migration and displacement across its colonial and postcolonial history, leading scholars to characterize it as a "refugee society" [34, 85]. After the Second World War, Hong Kong saw a large influx of migrants — numbering in the millions — fleeing political turmoil and socioeconomic instability in mainland China, many of whom settled permanently in the city-state [35, 64]. Moreover, between the mid-1970s and mid-1990s, Hong Kong served as a port of first asylum, for instance, for over 200,000 Vietnamese refugees, many of whom were later resettled in Western democratic countries like the United States, Canada, Australia, and France [65].

Migration has not been unidirectional; during the colonial period (1841 to 1997), the city experienced several waves of outward migration, driven by factors such as rural land dispossession in the New Territories in the 1950s and mounting uncertainty during the lead-up to the 1997 handover to the People's Republic of China. As a British colony, Hong Kong was embedded within broader transnational networks of mobility. However, since the handover, population growth has been driven primarily by migrants from mainland China, especially through family reunification schemes.

4.2 Emerging Hong Kong Diaspora After the 2019–2020 Protests

The 2019–2020 anti-extradition protests (AEP) marked a pivotal moment in Hong Kong's contentious politics, reviving large-scale mobilization after the 2014 Umbrella Movement. As many as 45.6 percent of the local population participated in the protests [21], and the reach of this unprecedented movement extended far beyond the streets through what became known as the "international front" [62]. This transnational dimension relied heavily on digital platforms, which facilitated the coordination of global solidarity actions and amplified Hong Kongers' demands on the world stage.

Everyday life during the protests became intensely politicized, with digital tools playing a key role in enabling new repertoires of resistance. Activists used online platforms for community organizing, political consumerism,[2] and real-time coordination [23]. As the state responded with the 2020 National Security Law and a wave of institutional restructuring, such as the overhaul of the electoral system and tightening of media control, these digital spaces became critical sites for both survival and dissent. The resulting atmosphere of repression and socio-political anxiety echoes similar collective emotions among the previous wave of mass migration in pre-handover Hong Kong [59].

Even as on-the-ground mobilization declined due to pandemic restrictions and state repression, the political energy of the social movement persisted online and across borders [47]. Mounting concerns over the erosion of judicial autonomy and the incompatibility of Hong Kong's legal system with mainland China's further fuelled political disaffection [18]. In the year ending June 2021, the city recorded a net outflow of 89,200 residents, the sharpest population decline in six decades [91]. A 2024 population survey conducted by the Chinese University of Hong Kong indicated that around 34.1 percent of respondents would choose to emigrate overseas if given the chance [92]. The top reasons cited included a bleak economic outlook, dissatisfaction with the undemocratic political system, ongoing political instability, and poor living conditions such as overcrowded housing [92].

This new wave of migration has drawn increasing attention to the making of a post-protest Hong Kong diaspora [34]. What distinguishes this diaspora from earlier waves is its deep entwinement with digital infrastructures [28, 94]. Through platforms such as Facebook, WhatsApp, Instagram, Telegram, and YouTube, Hong Kongers are building transnational networks of solidarity and collective memory, constructing and maintaining what can be understood as a "digital diaspora" [4, 81].

4.3 Hong Kong Diaspora in North America

North America has emerged as a key reference point for understanding the post-2019 Hong Kong digital diaspora. In both the U.S. and Canada, recent years have seen a visible increase in Hong Kongers relocating and establishing new forms of community, identity, and activism [90, 102]. These migrations are shaped not only by legal pathways and historical ties, but also by broader geopolitical shifts, such as the US-China rivalry and Canada's long-standing relationship with the pan-Chinese diaspora.

Importantly, digital platforms have become crucial infrastructures through which diasporic Hong Kongers maintain connections with each other and with those still in the city. From mutual aid groups on WhatsApp to advocacy campaigns on Facebook and political discourse on YouTube, the digital sphere functions as both a social lifeline and a site of struggle. Against this background, our study explores how diasporic communities in North America interpret political risk, navigate local conditions, and experiment with new forms of transnational belonging, highlighting both shared trajectories and place-based differences.

---

[2]Intentional purchasing or boycotting of products, goods, or services by citizens for political reasons, reflecting either a sense of dutiful citizenship or engaged citizenship [24].

5 Findings

5.1 Perceptions of Risk and Transnational Repression

Our findings reveal that diasporic Hong Kong identity is shaped by enduring perceptions of political, social, and economic risk, which are deeply rooted in prior experiences of repression. Following the materialization of direct state repression during the 2019 Anti-ELAB movement, there was an exodus, as many Hong Kong residents geographically relocated abroad, carrying with them a heightened awareness of ongoing threats. This collective memory of repression led to a persistent perception of transnational risks. These risks, amplified by digital connectivity, continued to structure diasporic life, community boundaries, and identity formation even after geographical relocation.

Building on Douglas and Wildavsky's [31] conceptualization of risk as a culturally constructed phenomenon and Slovic's [86] framing of risk perception as subjective, we define risk as a subjective assessment of potential harm, characterized by uncertainty and shaped by individuals' and collective interpretations and evaluations, which are informed by their contexts, experiences, and knowledge from past events. For Hong Kong diasporic communities, this subjectivity is further shaped by sociotechnical systems that amplify perceptions of harm and create patterns of shared concern. Although the distinctions between different categories of risk are often blurry, we identify five recurring types of perceived risk in our data.

5.1.1 Reputational Risk. Reputational risk refers to the subjective anticipation of losing social credibility or standing, driven by potential acts of misinformation, slander, or defamation. Importantly, in the context of coalition building and organizing, reputational harm can be particularly damaging, as it can fracture coalitions, provoke internal conflict, and undermine the legitimacy of organizing efforts. For example, Participant S11 recounted experiencing targeted slander on Golden, a Reddit-like Hong Kong forum, where fabricated rumours were used to undermine his political credibility, including insinuations about personal relationships and ulterior motives.

Reputational harm is not limited to individuals and extends to collective slander. Participant S04 recounted instances where members of their community were subjected to absurd and provocative accusations on platforms like Telegram, aimed at discrediting their political stance and causing disruption within the group.

> "(On Telegram) There are already multiple times where we spot blue ribbons came out of nowhere shouting ridiculous slogans like "You Yellow Ribbons support Bestiality and are being brainwashed". Not sure why they are shouting stuff like that. Brainwash fine but why Bestiality? it just doesn't make sense at all." - S04

A particularly potent form of reputational risk involves accusations of profiting from the social movement or from political suffering. The phrase "Steamed Buns Dipped in Human Blood" (人血饅頭) was often used to accuse organizations or individuals perceived as monetizing the movement. S04 described how this narrative is used to provoke moral outrage and fracture activist communities:

> "The term "Steamed Buns Dipped in Human Blood" in the legends means that you used your organization, the social movement, or a comrade as an excuse to make money. Honestly this is a curse, because a lot of artists actually just want to record an incident or let more people to understand the incident. Let me put it simply, Do you want those artist to make a lot of money, even if they are eating "Steamed Buns Dipped in Human Blood"? Or do you prefer the case where everyone doing protest artwork to not even able to pay for their meals? Of course you want everyone in the protest to be rich! come on!" - S04

5.1.2 Risk of "Sam Tau". *Sam Tau* (or 滲透) refers to the subjective anticipation of social conflict resulting from uncertain or changing political affiliations. *Sam Tau* is a Cantonese term, loosely translated as "diffusion" or "percolation," and captures the slow decay in solidarity, likened to water percolating through rock. Fear, as a consequence of uncertainty and concerns about political affiliations, causes social trust to gradually erode and decay over time and break the unity of a community from within. Eventually, *Sam Tau* ends in social fragmentation, where nobody knows who is trustworthy enough to form scalable resistance against the state. What makes *Sam Tau* alarming is its invisibility and informality; social conflict could arise without symptoms, with dire consequences, especially if unknowingly associating with antagonistic political affiliations.

S03 shared that within his family, discussions on political topics are avoided due to differing views and the fear of causing discomfort, illustrating the pervasive nature of *Sam Tau* even among close relatives.

> "One of my cousins is a teacher. And my another cousin a nurse. They will initially comment their dissatisfaction on healthcare system and the removal of liberal studies, but they could not leave Hong Kong. This is now their mindset, they cannot express themselves freely nor post freely. I of course understand they also faces many challenges, so I now refrain from talking about controversial topics with them too..." - S03

As *Sam Tau* is widely known to be a concern, to mitigate such risks, risk-aware diasporic organizers had to implement sociotechnical boundaries and control access to personal information among members of the group. Participant S04 shared that concerns over *Sam Tau* influenced his decision to avoid LinkedIn for community coordination:

> "I don't want to use LinkedIn because of the sensitivity problem, I don't want to be "Sam Tau" by people and get all our information stolen. This is very dangerous. We don't know whether we are being targeted, I won't be that conceited to claim that the CCP must target us, or the HKSAR Gov must target us, we are just a small organization, but still..." - S04

Generational tensions also surfaced; participants mentioned perceptions that, in contrast to the younger generation, the older generation were more susceptible to government news releases or propaganda. Participant S06 described a situation where a suggestion by an older community member to apply for Hong Kong government funding led to tensions with younger members, who felt that accepting such funding contradicted their reasons for relocating.

The risk is further complicated by the affordances of digital platforms, where anonymity and scale obscure shifts in political stance. S11 shared a personal experience in which a private post on Facebook, critical of police and intended only for friends, was screenshotted and shared publicly by someone on his friend list. This incident, which he described as a betrayal, revealed how easily digital intimacy can be breached and highlights the difficulty of discerning trusted affiliations in online spaces.

5.1.3 Infiltration Risk. Infiltration risk is a subjective anticipation of organizational disruptions or internal sabotage through potential infiltrators. It is a recurring concern in diasporic organizing, particularly where trust is foundational but difficult to verify. For example, S07 noted that even referral-based organizations are not immune to infiltration, as past incidents have shown that individuals can still cause disruptions despite initial vetting processes.

> "Even if there is a referral, your risk mitigation doesn't imply there is no risk, it's just that you minimize the risk. As for the membership to our organization, it is because there were cases happened before that someone came in and caused troubles. That was before me but I have heard stories about it." - S07

These anxieties extend to long-standing diaspora institutions. S11 described how an Overseas Chinese Association with decades of democratic advocacy history was infiltrated and co-opted as an agency of the Chinese embassy.

> "A friend … visited one of the overseas Chinese association that has already been "reddened (赤化)", but he was the chairman of the organization so he had to go despite he knew the change of the association. After his visit, he shared with me how the Chinese Embassy representatives there asked him to relay their greetings to me." - S11

5.1.4   State Surveillance. State surveillance risk is a subjective anticipation of state-driven repression involving uncertainty around surveillance methods, infiltration, cyber-attacks, and coercive state actions. While oftentimes this risk was obvious and had direct traces to state-driven repression, more indirect state-driven repression was unfortunately less discernible.

Participant S11 cited the high-profile case of a Hong Konger prosecuted for incitement because she liked a pro-democracy Facebook post while studying in Japan.

> "Previously a girl liked a post during her study in Japan and was prosecuted for offence of incitement when she returned to Hong Kong. No joke, the case is just for liking a post and sharing in Japan. That girl was studying in Japan, liking and sharing the post in Japan, only return to Hong Kong to change her Hong Kong passport and was prosecuted retroactively…" - S11

Participant S07 mentioned that everything is being surveilled and that, due to uncertainty about technology and the state's capacity, people should always assume the state is "all knowing."

> "If you are not doing something that [the state] wants you to do, the risk is already there. No matter whether if you are just pressing a few likes on Facebook, promoting something or saying something, or being with certain people or taking pictures with someone, everyone has risk and it might just be you. No one could tell you where the risk is, you always assume there is risk no matter what. You have to assume that he is all knowing. You have got liability on event preponderance of evidence" - S07

5.1.5   Non-state surveillance. Non-state surveillance is a subjective anticipation of professional harm through surveillance-like practices by non-state entities. It is the most pervasive risk, as it could happen anywhere and anytime. This includes employer surveillance, nationalist "Little Pink" networks, and algorithmic profiling.

Participant S07 explained his avoidance of protests due to fears of being targeted by Chinese nationalists abroad, also known as the "Little Red Pink," who engage in nationalistic behaviour, often hostile to anyone speaking negatively about China. However, despite S07's intentional avoidance, the pervasiveness of non-state surveillance led to him being surveilled in his workplace by his colleagues.

> "During the time of social movement, I was working in a high-tech firm and many people asked what happened to Hong Kong. So I wanted to organize an informal gathering to explain what happened in Hong Kong. Then all of a sudden, I got complained by someone to the HR. The HR came and tap me on my shoulder telling me not to do it here, like a friendly reminder … I was shocked by the fact that someone complained." - S07

The above forms of non-state surveillance are very obvious in that the actors doing the surveilling are identifiable. However, participants often expressed concerns that the origin of non-state surveillance could be more discreet, even operating ambiently through digital infrastructure. Participant

S03 described the fear of non-state surveillance through everyday services like travel agencies and highlighted concerns about identity theft and espionage:

> "For example, Hong Kongers like to go to travel. If a Chinese spy worked for the famous Hong Kong travel agency and steal our identity information, we would be doomed. Canada is a relatively democratic country, so these privacy breaches is rather concerning, especially in the case of identity theft and those self-proclaim Hong Kongers who abuse the identity and act as spies in another country." - S03

Related to *Sam Tau*, S06 also shared concerns about friends' political affiliation, especially friends who continued to reside in Hong Kong and were subject to the National Security Law. In cases where her friends' political affiliation has shifted or when a conflict of interest arises, her digital traces and communication records pose a risk of potential non-state surveillance.

> "One of the reasons is afraid of leaving traces and records. Another reason being the friends who work in Hong Kong, their political stance may have already changed, not sure how they perceive things, so avoidance on this topic is an avoidance of conflicts among friends that will harm the friendship." - S06

These risk perceptions, deeply intertwined with experiences of political repression and cultural displacement, are not only socially shared but also technologically mediated.

5.2 Tech-Mediated Risk, Identity and Organizing

We find that technology both enables diasporic organizing and amplifies the risk of transnational repression. Across our data, participants described how technologies simultaneously fostered solidarity, allowing a transnational Hong Kong identity to emerge, while also imposing new vulnerabilities. This section presents how the diasporic Hong Kong community perceive and engage with technology in their everyday organizing practices, and highlights three interrelated dynamics: (1) how technology contributes to perceptions of risk; (2) how technology facilitates the construction of a risk-aware diasporic identity; and (3) how technology enables the scalability of organizing efforts across the diaspora.

5.2.1 Technology and Perception of Risk. Perceptions of risk are shaped by the affordances and opacity of digital technologies. Many participants described a sense of uncertainty when engaging with platforms widely associated with state surveillance, a perception compounded by users' lack of digital knowledge and/or feeling coerced into technological dependencies by institutional or professional demands.

For example, participant S01, a university-educated young professional, expressed both technical uncertainty and limited capacity to mitigate digital risks. However, despite knowing potential risks, he described feeling compelled to use apps like WeChat and Little Red Book due to his work responsibilities, highlighting the structural coercion many diasporic actors face:

> "... I really do not want to (download WeChat) in the early days but sometimes there is no choice, because at the end of the day my work needs it. I also don't want to download Little Red Book but I really have a working need. Some evidence by the client is actually on Little Red Book, can't escape because my job really needs it. The risk is therefore unavoidable..." - S01

This structural coercion into transnational repression is amplified through platform design, in this case, the referral requirement. After S01 reluctantly consented to using the app, WeChat required him to reach out to his social network for a guarantor in order to continue his account registration.

> "When you need to register for an account (on WeChat) there is a form of collective punishment, which means you need to have referrals from friends or family in order to open an account. You kind of help the people who monitor your life to understand your social circle...That time I also want to do some preventive measure to avoid my family to be forced to use WeChat because of them (workplace). I worry about the safety risk so I don't want to do this..." - S01

It is evident that these digital infrastructures are designed in ways that condition individuals to tolerate both technological opacity and constant surveillance. Such design enables technology to permeate geographical and social boundaries, compounding users' perceptions of risk and deepening their sense of insecurity.

5.2.2 Technology in Constructing a Risk-Aware Hong Kong Identity. The collective vulnerability to isolation in the diaspora and the collective perception of risk that persisted after the social movement and followed into the diaspora have led to the emergence of a risk-aware Hong Kong identity. In the face of transnational repression and the challenges of living in a new environment, our data captured the process of how diasporic Hong Kong communities are constructing identities and creating boundaries through technology and gatekeeping practices. Participants S01 and S06, both recent immigrants residing in the diaspora for less than two years, shared their experiences of accessing diasporic Hong Kong communities through technology and the reasons they chose to join.

> "In terms of platform then Instagram, Telegram, or earlier then a bit more Facebook... I can't precisely recall but the main entry point is perhaps church or interests group such as chess, badminton, boardgames, and etc. Other entry point perhaps would be university alumni association. Mainly to collect information, of course there are also a small amount of immigration information group to understand everyone's immigration processing time..." - S01

> "Many wanted to build a network. Because a lot of times many people did not come here with friends or family, they will want to make some friends, this is why they will join these WhatsApp group to see if it is possible to build relationships with Hong Kongers. I think mainly is this reason...." - S06

As previously shown, isolation in the diaspora is a main driver of community organizing. However, there was a certain urgency and exclusivity in these networks that reflected deeper, more implicit concerns. Beyond cultural familiarity, the desire to connect specifically with diasporic Hong Kongers and form enclaves — something that did not happen in prior waves of migration — signals an emerging political identity driven by perceived threats. Our findings show that this selective networking was less about nostalgia and more about creating a protective enclave, i.e., a community of shared understanding and trust in the face of external risks. For example, within just two years of arriving, S01 and S06 had not only joined but also organized local gatherings in diasporic Hong Kong communities through social media channels.

5.2.3 Technology in Scalable Diasporic Organizing. Technology also plays an important role in the scalability of diasporic organizing. Participants described continuing practices from the 2019 movement, where secure messaging apps and social platforms, such as Signal and Telegram, were instrumental to coordination and information dissemination. These technologies persist in the diaspora, facilitating both horizontal and vertical scaling of community efforts.

Participant S04 explained how communication protocols established during the movement were still in use:

"I use Signal. Usually we continue the rules where small group (N<=3) uses Signal and large groups (N>3) uses Telegram. But now Signal has changed and are allowed to block phone number so either Signal or Telegram it doesn't matter. But Telegram I have already been using it. So it's more convenient..." - S04

Participant S06 echoed this continuity, noting how secure platforms were adopted early on due to concerns about privacy:

"Signal and Telegram should be during the time of occupy central movement because that was the time when more people recommend communication software beyond Whatsapp. People think that these apps are safe and not easy for people to collect your information, this is why I downloaded them...." - S06

Given the difficulty of in-person communication, participants also described tailoring their platform choices to audience reach, often keeping generational preferences in mind. Participant S08 noted a strategic shift towards using Instagram for outreach, recognizing its popularity among younger generations and its effectiveness in disseminating information within the community. Further, at the organizational level, tools like WhatsApp and Google Drive facilitated backend coordination for formal organizations such as chambers of commerce.

As these findings suggest, scalable diasporic organizing among Hong Kong communities, from student networks to professional associations, is largely enabled by social media and messaging apps, with their use shaped by both diasporic isolation and perceptions of risk. These platforms were adopted based on popularity, perceived digital risks inherited from the social movement context, and their potential outreach to a specific group of target audiences. However, the boundaries of these audiences are often ambiguous, and it is difficult to assess the true scalability of these technologies. These collective practices, mediated through digital infrastructures and shaped by diverse risk perceptions, form the basis of a complex and evolving risk landscape.

5.3 Risk Mitigation Strategies

Having established that risk is central to diasporic Hong Kong identity and organizing, we now turn to examine how members of this diaspora attempt to navigate, mitigate, or manage these risks. Participants in our study engaged in a wide array of risk mitigation strategies, many of which were improvised, socially learned, and context-specific. These strategies function less as definitive solutions and more as adaptive responses shaped by past harms and present uncertainties.

5.3.1 Platform Selection and Non-Use: Platform selection, both in terms of adoption and avoidance, was a widespread risk mitigation strategy among our participants. In general, participants sought to avoid or minimize "risky" platforms associated with surveillance or misinformation, or shifted to lower risk spaces (digital or offline). Deliberate avoidance of platforms such as WeChat — due to their perceived ties to Chinese state surveillance — was a widely adopted strategy among participants, except when professional obligations necessitated their use.

In order to mitigate risk stemming from communication through digital platforms, our participants employed a range of precautionary practices depending on the threat contexts. Several tailored their choices according to correspondent sensitivity, like S11, who exclusively used ProtonMail for high-risk contacts while avoiding Google Drive entirely. Others, including S06, based platform selection on content sensitivity, preferring Signal over WhatsApp for transmitting sensitive documents like personal IDs, which were promptly deleted after use.

Beyond content and contact considerations, participants also leveraged platform affordances for vetting purposes and curating community participants. As S04 highlighted,

> "We will check their background because the only way to join the network is Facebook.
> I will check their entire Facebook history, like what time did they open the account,
> what sort of posts and comments are there, did they post any slogans? It is on this
> foundation that I met many comrades." - S04

Furthermore, participants also employed identity management as a key tactic, though implementation varied by technical literacy and risk perception. For example, S06 maintained separate anonymous YouTube accounts for accessing political content, deliberately devoid of personal identifiers to ensure safe viewing across jurisdictions, whether in Hong Kong or Canada. More tech-savvy participants like S07, drawing on professional risk assessment skills, used extensive digital compartmentalization — maintaining distinct communication channels (Signal, Telegram, Discord, LinkedIn, WhatsApp) with separate identifiers for each platform while avoiding WeChat entirely.

As previously mentioned, to minimize surveillance risk, both state and non-state, many participants shared a continued reliance on secure messaging platforms like Signal and Telegram, a practice carried over from the 2019 Anti-ELAB movement. As S04 explained:

> "At that time, the industrial standard of yellow circle is that when the group has more
> than three people then use TG, less than three people then use Signal. We still use this
> strategy, small group use Signal. Large group use TG. The good thing about TG is that
> you could block the phone number and change any name." - S04

This strategic continuity demonstrates how protest-tested security measures become institutionalized within at-risk communities facing ongoing repression. Moreover, it reveals a community-derived standard for secure communication: using Signal for small, trusted groups and Telegram for larger groups and its identity-masking features.

5.3.2 Self-censorship and Identity Management. Participants frequently employed self-censorship and modulation of text as strategies to reduce exposure to both state and non-state surveillance. These tactics included avoiding sensitive language, withholding identifiable information, and modulating political expressions depending on audience.

For instance participant S04 described his personal guideline for excluding explicitly political slogans from marketplace products, citing customer safety as the rationale:

> "I made it clear with the vendor in black and white. If there are wordings like Hong
> Kong Independence, Liberate Hong Kong, Revolution of Our times, I won't sell it.
> Honestly, in another extreme, if they said Long Live Xi, I love Hong Kong, those I also
> won't sell." - S04

S04 further highlighted the risk associated with anonymity, where "everyone is just a username." In response to infiltration risks, S04 maintained strict identity boundaries, and removed anyone who he thought was "suspicious." Other participants maintained multiple accounts to manage identity exposure.

Participant S11 described how one could protect themselves when delivering sensitive messages through the use of humour or verbal irony, citing the examples of high-profile pro-democracy YouTubers who appropriate pro-regime rhetoric in their daily content production.

5.3.3 Verifying/Filtering Information. Given the critical relation between online information and acceptance in diasporic Hong Kong communities, information verifying and filtering were widely adopted to actively reduce misinformation. Participant S11, with experience in news media, emphasized relying on academic and English-language sources to ensure the credibility of information, while deliberately avoiding Chinese-language sources. Participant S08, who operates a student-run news media platform, reflected on the difficulty of verifying information about events in Hong

Kong from within the diaspora and emphasized concerns about the authenticity of received content, highlighting broader challenges in establishing credibility in diasporic news production. However, while participants were aware of misinformation risks and sought to verify content, they often lacked effective strategies and remained uncertain about the reliability of their efforts.

5.3.4   Gatekeeping and Socio-technical Vetting. One of the most significant responses to risk was through gatekeeping and vetting practices. These serve to manage uncertainty, maintain community integrity, and delineate trustworthy participants, especially in digital environments where social cues are mediated through technology. Further, these practices not only protect against external threats but also actively constitute and reinforce a shared diasporic identity.

Cultural Gatekeeping Practices. Participants described leveraging cultural familiarity as a form of informal authentication in diasporic social networks. Cultural gatekeeping practices allowed individuals to differentiate insiders — those who shared linguistic, culinary, and value systems rooted in Hong Kong — from potential outsiders whose unfamiliarity raised concerns about social trust.

One of the participants (S07) highlighted how everyday cultural elements such as pop culture, culinary traditions and shared values, served as intuitive signals of belonging:

> "Hong Kong has a special culture. For example we embrace freedom as a value till the point where we equate the Hong Konger identity with freedom. There are also things like Cantonese pop culture, Cantonese songs, and the most important food culture. All Asians love food and Cantonese speaking people particularly loves to drink soup..." - S07

Participant (S02) shared more subtle markers, for example, people from Hong Kong emphasizing a lot of efficiency:

> "For example the timeliness to prepare food ... the attitude of the waitress and the workflow all emphasizes on efficiency. If you go to a western restaurant, there will be a lot of conversation and greetings, Hong Kong waitress don't often do that." - S02

Participants also stressed that cultural belonging was not determined solely by birthplace or citizenship status. Participant (S06), for example, described a definition of being a Hong Konger that related to spending enough time immersing oneself in Hong Kong culture:

> "If I must define Hong Konger, it would be the people who have resided in Hong Kong for long enough to understand the Hong Kong culture and have assimilated into the society, perhaps they are basically the same as everyone aside from their accent, then I would consider those people Hong Kongers..." - S06

Cultural gatekeeping allowed diasporic communities to construct and expand social networks grounded in a shared sense of Hong Kong identity. While an important and necessary line of defence against perceived risks, it was insufficient to address forms of vulnerability that were related to transnational repression, surveillance, and the collective suffering rooted in being part of the Hong Kong social movements. An additional layer of verification, based on political alignment and history, was required.

Political Gatekeeping Practices. Political gatekeeping emerged as a response to more direct and targeted risks, such as infiltration and state surveillance. These forms of gatekeeping were designed to ensure that only those with demonstrable commitment to the pro-democracy cause, shared histories of political struggle, and experiences similar risk of repression were trusted as insiders.

One of the participants (S04), a diasporic community organizer outlined the use of digital traces in political gatekeeping, emphasizing political engagement, consistency, authenticity, and intent.

> "I will ask questions like to determine whether you are a yellow ribbon like can you
> list the three slogans or name the incidents that happened. I will then check their
> Facebook history. For instance, accounts opened after 2019 I usually won't add them
> into the group because they are usually fake accounts. The other thing is if you have
> a long history but you deleted all the post on your profile, I'm sorry but this is also
> unacceptable..." - S04

In political vetting, consistency over time — demonstrated through digital traces, past activism, or long-term engagement — was often treated as a marker of authenticity, where authenticity is often a determining factor in an individual's acceptance into the community. As S03 explained:

> "If you are talking about engagement with the community, the Hong Kong Umbrella
> Movement is a lot more engaging to me because I have been very sensitive about events
> in Hong Kong since the time of Tung Chee-hwa (1997), it is after all my root..." - S03

Compared to cultural gatekeeping, political gatekeeping emphasized ideological consistency and the need for higher levels of confidence. In an environment characterized by fear of surveillance, sabotage, and shifting allegiances, political vetting practices became essential for sustaining trust within the diaspora. These practices simultaneously protected the community against external threats and reinforced the sense of a politically defined, risk-aware diasporic identity.

Digital Traces and Identity Curation. Digitally, gatekeeping practices operate primarily through the traces that individuals leave behind on platforms like Facebook, Instagram, Telegram, and YouTube. These traces are used both passively (as indicators of political or cultural affiliation) and actively (through profile checking and background verification).

As the entry point into the diasporic Hong Kong community is often through digital platforms, digital traces that demonstrate an authentic background from Hong Kong is almost a prerequisite to be included in the diasporic Hong Kong circle, as explained by participant S11:

> "Some people are called "acquaintances", which means you have to add them by courtesy,
> but you don't actually want to show them your post. So all my posts are set to "except
> acquaintance" and this is a security setting I would do. Sometimes there are also people
> reminding me not to say something so you could only see me talking about something
> that is related to my daily life and won't talk too much about politics." - S11

Maintaining boundaries in hostile environments requires constant awareness. As digital platforms have become primary entry points into diasporic Hong Kong communities, digital traces, and efforts to control or curate them are central to both trust-building and risk mitigation.

These layered gatekeeping mechanisms directly address several of the perceived risks outlined earlier — including reputational harm, infiltration, *Sam Tau* (滲透), and both state and non-state surveillance. In contexts where formal trust mechanisms are absent and digital interactions dominate, sociotechnical vetting becomes the basis of community inclusion. Peer assessments of credibility, though ambiguous and socially variable, remain a necessary defence and a key component in constructing a politically defined, risk-aware diasporic identity.

6 Discussion

This paper has examined how diasporic Hong Kongers navigate risk in their everyday lives, and how such risk is entangled with technologies, social relationships, and collective identity. In this landscape, risk does not operate in isolation but is mediated and amplified through sociotechnical systems within which diasporic actors are embedded. We identified five interrelated forms of perceived risk — reputational harm, *Sam Tau* (滲透), infiltration, state surveillance, and non-state surveillance — each exemplifying how vulnerability can be produced not only through explicit

repression but also through uncertainty and fear. Technologies such as Telegram, Signal, Facebook, and WhatsApp are consequently also used for gatekeeping, vetting, and boundary negotiation. At the same time, diasporic actors strategically repurpose these platforms to construct digital enclaves, cultivate a coherent political identity, and organize across geographies.

These findings present unique challenges to CSCW researchers studying transnational contexts and social movements, and we make the following three key contributions. First, we examine how collective identity is constructed through shared vulnerabilities and sociotechnical practices of risk management. Second, we revisit longstanding commitments in CSCW and HCI to transparency, openness, and inclusion, suggesting that these principles require rethinking in contexts where visibility entails danger. Third, we explore how diasporic organizers leverage and reshape sociotechnical infrastructures to sustain organizing under repression, offering implications for the design of technologies that better support diasporic organizing under transnational repression.

6.1 Risk, Technology, and Collective Identity

Across our findings, risk emerges as an active structuring force that shapes the contours of collective identity, community, and technology use. For Hong Kong diasporic actors, risk is not just about the presence or absence of transnational repression; rather, it saturates their everyday lives and modulates both social relationships and technology use. This ambient condition of risk, historically situated in the experience of direct repression during the Anti-ELAB movement, is experienced by the diaspora through sociotechnical infrastructures. Here, we suggest that this risk operates as a binding force shaping collective identity: a latent yet organizing logic through which diasporic subjects come to recognize one another, assert political affiliation, and negotiate inclusion.

The recognition of shared risk produces a particular diasporic sensibility — one that is inherently political, curated (rather vigilantly), and technologically mediated. Technologies such as Telegram, Signal, and Facebook are not just communication tools; they are spaces within which these diasporic identities are enacted, contested, and authenticated. It is through these platforms that participants gauge reputational standing, trace political affiliations, and enact gatekeeping practices that sort potential community members into (subjective) gradients of trustworthiness. These practices are less about ensuring absolute security and more about generating collectively legible signals of intent, belonging, and subsequently, assessments of risk. Risk, then, can be considered a semiotic system through which diasporic actors read each other.

Importantly, our participants' careful curation of digital traces — from pseudonymous accounts to selective platform engagement — speaks to a form of diasporic identity work that is inherently (and pre-emptively) defensive. While conventional understandings of diasporic identity often assume self-assertion [1, 41], here we see identity constructed through withdrawal, concealment, and controlled visibility. Digital technologies thus play two roles: they can be instruments of recognition and connection, as well as exposure and suppression. Under such conditions, the collective is not bound by just shared values, but by the mutual recognition of vulnerability.

Furthermore, our participants also reported feeling compelled to use applications such as WeChat and Little Red Book due to professional obligations. Prior studies have noted that platforms like WeChat — having become infrastructural for the Chinese diaspora — serve purposes beyond communication, including financial transactions, business operations, and client management [104]. This suggests that complete risk avoidance through platform abstention is often unfeasible for diaspora members, even when community members are cognizant of surveillance risks and transnational repression when engaging with platforms and technologies that have linkages with host societies' state apparatus. Therefore, CSCW needs to explore how diaspora communities navigate digital risks when participating in transnational social movements, examining both (1)

their dependencies on digital infrastructures under repressive conditions, and (2) design implications for such sociotechnical contexts.

As shown in the findings, the interplay of risk, identity, and technology leads participants to selectively gravitate toward digital enclaves [29, 33, 106] of cultural and political familiarity. In these risk-aware communities, identity is a distributed social infrastructure that manages the precarity of diasporic life under watchful regimes. Our study adds to CSCW's growing attention to the affective and political dimensions of sociotechnical infrastructures, particularly in contexts marked by repression, displacement, and collective insecurity.

6.2 Contextualizing Risk and Rethinking Visibility/Openness

Current conversations on transnational repression have focused on state-backed spyware, digital coercion, and algorithmic profiling [26, 42, 73, 96]. While these mechanisms remain central to the exercise of power, our findings suggest that the threat landscape is far broader and more indeterminate. The most pervasive risks are not solely from distant state technologies but from uncertainty itself: the inability to ascertain a person's political allegiance or affiliation and the fear of silent/pervasive/informal non-state surveillance. Risk mitigation, in this setting, is not merely a matter of individual protection, but a communal and often collaborative project. Notably, the risk calculus is not limited to personal threat models, but distributed across historical experience, relational proximity, and political alignment.

In this context, we extend Nissenbaum's theory of contextual integrity [75, 76] to argue that risk itself may be better conceptualized as a contextual norm[3] that is socially situated and defined by collectively held expectations about safety, visibility, and legibility within particular sociotechnical and sociopolitical ecologies.

This lens yields critical implications for CSCW researchers designing technologies with and for diasporas facing transnational repression: (a) it requires a commitment to context mapping of diasporic ecosystems and their digital-territorial relations and ambiguities; (b) it necessitates the documentation and design of community-developed risk epistemologies (e.g., vetting protocols and processes); and (c) it demands a methodological stance that traces coercive or disruptive flows from both state and aligned non-state actors. Together, CSCW and design need to move beyond the technical apparatus of surveillance and privacy to the relational infrastructures through which risk is perceived, mitigated, and collectively endured by diasporic participants facing transnational repression.

Furthermore, the practices of gatekeeping, as evidenced in the findings, highlight a certain kind of boundary work (for risk mitigation) which does not align with the long-standing assumptions in CSCW and social computing about openness, inclusion, and democratic participation [45, 60, 61]. Historically, CSCW has emphasized the design of systems that foster collaboration, enable information flow, and democratize participation across distributed contexts [12, 61]. Such a normative orientation toward openness and transparency does not take into account instances where visibility and openness entail existential risk, and where exclusion is not incidental but integral to the preservation of communal trust and political safety.

Prior CSCW work has used the metaphor of the panopticon to examine how visibility and control are enacted in sociotechnical contexts, such as crowdwork[52], bureaucratic systems[97], open-source collaboration[51], and domestic life[13]. These studies, however, typically conceptualize panopticons as locally bounded sociotechnical systems affecting one domain of societal life, often

---

[3]Nissenbaum's theory of privacy as contextual integrity [75, 76] frames the need for privacy protection as being attentive to the norms governing specific social contexts. Hence, public surveillance constitutes an injustice because it violates this contextual integrity.

bracketing the active role of the state in producing, sustaining, and extending panoptic visibility. Our study extends this perspective by conceptualizing the state itself as a panoptic formation in which politically marginalized diasporas must navigate a transnational surveillance system where multiple forms of risk interplay. In our analysis, the panoptic gaze appears not as a single apparatus but as a diffused constellation of mechanisms through which state power circulates across borders, compelling communities to navigate, subvert, or resist state-led surveillance. At the same time, our study shows how this panoptic gaze is internalized by participants, reconfiguring everyday practices of self-censorship, boundary drawing, and cautious representational management. This conceptual shift underscores how invisibility can be purposeful and how visibility is not always beneficial, especially for marginalized communities seeking to evade the panoptic gaze of a state[19]. Our study extends this frame to highlight the specific burdens placed on politically marginalized diasporas in the face of transnational repression.

6.3 Organizing and Tech Infrastructures

While current discussions of transnational repression focus on state-based coercive tactics and their operationalization through digital infrastructures, these accounts tend to frame non-state actors as instruments operating at the behest of authoritarian regimes [37, 70]. Our findings, however, reveal a more nuanced picture: participants described transnational repression not just as a threat to bodily safety or legal security, but also as a condition that erodes the very social fabric of diasporic life. Repression thus materializes and operates through more diffuse mechanisms of relational uncertainty that delegitimize dissent and force a culture of self-censorship among diasporic communities.

Therefore, we argue that transnational repression should be understood as part of authoritarian surveillant assemblages [95] — dynamic networks of interconnected surveillance systems that continually expand in scope, forge new connections, and integrate diverse actors. These surveillant assemblages entail vectors of risk that extend beyond persecution by the state itself, and these configurations are neither fixed, linear, nor uniform. Components and actors evolve through ongoing processes of adaptation and transformation. This insight is particularly critical for the CSCW community. Conventional security paradigms premised on formalized adversarial structures are inadequate for capturing the relational and distributed dynamics of diasporic organizing under repression. Instead of centralized moderation or centralized threat identification, there is a need for decentralized and adaptive, context-sensitive systems of trust and reputation, alongside design features that enable diasporic subjects to contest and reinterpret retroactively imposed identifications or categorizations.

Our findings extend prior CSCW literature on community moderation [5] and organizational vetting [56, 67, 71] by showing how gatekeeping and vetting emerge not as formalized institutional mechanisms, but as everyday sociotechnical practices embedded within the uncertainties of transnational repression (from both state and non-state entities). These practices aim to preserve movement identity, ensure goal alignment, and maintain the cohesion in community building and of political messaging. Importantly, community gatekeeping is not merely a technological process; it is also shaped by identifying cultural anchoring and cues of participants and informed by histories of political participation.

In this context, digital traces play a crucial role. Notably, the dialectical relationship between digital traces and identity curation is central to this dynamic. While digital traces can expose individuals to surveillance and repression by state actors, they simultaneously serve as essential resources for maintaining trust, establishing legitimacy, and boundary maintenance within the social movement. Trust, under such conditions, must be continually enacted, reassessed, and socially distributed.

Therefore, the sociotechnical practices of vetting, as we show in this paper, are neither fully algorithmic nor entirely interpersonal, but instead situated enactments that draw from past political memory, present uncertainties, and the affordances of platforms. Messaging platforms such as Telegram and Signal, beyond tools for coordination, are sites where community boundaries, political solidarities, and strategies of mutual care are enacted. The continued reliance on these platforms, many of which were adopted during the 2019 Anti-ELAB movement and subsequently normalized in diasporic settings, is a consequence of both their technical affordances and their retention of a memory of political survival in the face of repression.

Design for such forms of diasporic organizing must begin from the recognition that engagement with technology is almost always shaped by perceptions of risk. These perceptions are not static, rational, or objective assessments; rather, they emerge from geopolitical context, social history, and mediated experience. Often, for diasporic Hong Kongers, it is not whether risk is present or absent, but how it might be latent or obscured. Design should thus look beyond discrete threat models or predefined privacy settings and treat risk as an ongoing process of sensemaking and adaptive boundary maintenance. In this context, organizing infrastructures must be designed not merely for coordination or mobilization, but for trust curation, selective visibility, and signalling. As such, organizing under transnational repression challenges CSCW to consider sociotechnical infrastructures as dynamic and politically entangled forms that are co-produced with social imaginaries of risk, solidarity, and resistance.

Designs for communities facing transnational repression must also be attentive to culturally sensitive onboarding processes for technology and platform use, reputation identification systems, and mechanisms for visibility. These features must navigate enduring tensions, such as trade-offs between scalability and high privacy, and move beyond transparency and participatory reach toward supporting trust curation, community-led risk assessment, and adaptive or selective visibility controls. Such considerations are particularly urgent in the current geopolitical moment. As authoritarian regimes increasingly extend their reach through digital infrastructures, diasporic communities are reconstituted as sites of both vulnerability and resistance. Designing for these conditions is not only a sociotechnical or organizational challenge, but an ethical and political necessity.

7 Conclusion

Diasporic Hong Kongers navigate risk in their everyday lives as a subjective, relational, and sociotechnical construct, shaped by the ongoing presence of transnational repression. However, the diaspora's experiences of these risks extend beyond encounters with state-driven vectors, such as state surveillance, and also along other axes — including reputational harm, "Sam Tau" (滲透), infiltration, and non-state surveillance — each modulating the rhythms of their social lives, political organising, and technology use. This diasporic sensibility is inherently political but also curated through adaptive socio-technical practices such as gatekeeping community spaces, sociotechnical vetting, self-censorship, identity management, and engaging in cautious platform selection or non-use. These practices reflect the diaspora's response to a multidimensional risk calculus posed by transnational repression, unfolding through what we understand as authoritarian surveillant assemblages.

As our study reveals, Hong Kong diasporic organizers seek to preserve movement identity, ensure goal alignment, and maintain cohesion through digital enclaves and selective participation. Notably, for the Hong Kong diaspora, withdrawing from the normative anchoring of virtues such as openness and transparency, or defining exclusion, is not incidental but rather integral to preserving communal trust and political safety. This insight is critical for CSCW and HCI scholars: designing with and for diasporas under repression requires a risk-aware orientation that begins with the

recognition that engagement with technology is almost always shaped by perceptions of harm, ambient uncertainty, and situated histories of repression. Our work calls for more contextually grounded and politically responsive design practices that can better support diasporic social movements navigating transnational repression.

Acknowledgments

References

[1] Fiona Adamson. 2012. Constructing the Diaspora: Diaspora Identity Politics and Transnational Social Movements. *Politics from afar: Transnational diasporas and networks* (2012), 25–42.

[2] Shane Ahern, Dean Eckles, Nathaniel S Good, Simon King, Mor Naaman, and Rahul Nair. 2007. Over-Exposed? Privacy Patterns and Considerations in Online and Mobile Photo Sharing. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. 357–366.

[3] Noura Al-Jizawi, Siena Antis, Sharly Chan, Adam Senft, and Ronald J Deibert. 2020. Digital Transnational Repression. *Citizen Lab* (2020).

[4] Andoni Alonso. 2010. *Diasporas in the New Media Age: Identity, Politics, and Community.* University of Nevada Press, Reno.

[5] Tawfiq Ammari, Momina Nofal, Mustafa Naseem, and Maryam Mustafa. 2022. Moderation as Empowerment: Creating and Managing Women-Only Digital Safe Spaces. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2, Article 313 (Nov. 2022), 36 pages. doi:10.1145/3555204

[6] Anas Ansar and Julian Maitra. 2024. Digital Diaspora Activism at the Margins: Unfolding Rohingya Diaspora Interactions on Facebook (2017–2022). *Social Media+ Society* 10, 1 (2024), 20563051241228603. doi:10.1177/20563051241228603

[7] Sarah Armouch, Reem Talhouk, and Vasilis Vlachokyriakos. 2022. Revolting From Abroad: The Formation of a Lebanese Transnational Public. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–28.

[8] Kagonya Awori, Frank Vetere, and Wally Smith. 2015. Transnationalism, Indigenous Knowledge and Technology: Insights From the Kenyan Diaspora. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. 3759–3768.

[9] Andrew Besmer and Heather Richter Lipford. 2010. Moving Beyond Untagging: Photo Privacy in a Tagged World. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 1563–1572.

[10] Michael L Best, Thomas N Smyth, Daniel Serrano-Baquero, and John Etherton. 2009. Designing For and With Diaspora: A Case Study of Work for the Truth and Reconciliation Commission of Liberia. In *CHI'09 Extended Abstracts on Human Factors in Computing Systems*. 2903–2918.

[11] Sophie Bishop. 2021. Influencer Management Tools: Algorithmic Cultures, Brand Safety, and Bias. *Social media+ society* 7, 1 (2021), 20563051211003066.

[12] Pernille Bjørn and Nina Boulus-Rødje. 2015. The Multiple Intersecting Sites of Design in CSCW Research. *Computer Supported Cooperative Work (CSCW)* 24 (2015), 319–351.

[13] Julie Boesen, Jennifer A Rode, and Clara Mancini. 2010. The Domestic Panopticon: Location Tracking in Families. In *Proceedings of the 12th ACM international conference on Ubiquitous computing*. 65–74.

[14] Asa Boholm. 2015. *Anthropology and risk.* Routledge.

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

[16] Jennifer M. Brinkerhoff. 2009. *Digital Diasporas: Identity and Transnational Engagement.* Cambridge University Press, Cambridge New York.

[17] Patrick Brown. 2017. *Theories of uncertainty and risk across different modernities.* Routledge London.

[18] Yuk Wah Chan and Yvette To (Eds.). 2025. *Global Hong Kong: Post-2019 Migrations and the New Hong Kong Diaspora.* Routledge, Abingdon, Oxon New York, NY. doi:10.4324/9781003544159

[19] Priyank Chandra. 2017. Informality and Invisibility: Traditional Technologies as Tools for Collaboration in an Informal Market. In *Proceedings of the 2017 chi conference on human factors in computing systems*. 4765–4775.

[20] Karma R Chávez. 2011. Counter-Public Enclaves and Understanding the Function of Rhetoric in Social Movement Coalition-Building. *Communication Quarterly* 59, 1 (2011), 1–18.

[21] Edmund W Cheng, Francis LF Lee, Samson Yuen, and Gary Tang. 2022. Total Mobilization From Below: Hong Kong's Freedom Summer. *The China Quarterly* 251 (2022), 629–659.

[22] Wilfred M Chow and Dov H Levin. 2024. Muddying the Waters: How Perceived Foreign Interference Affects Public Opinion on Protest Movements. *American Political Science Review* (2024), 1–18.

[23] Hiu-Fung Chung. 2020. Changing Repertoires of Contention in Hong Kong: A Case Study on the Anti-Extradition Bill Movement. *China Perspectives* 2020, 2020-3 (2020), 57–63. doi:10.4000/chinaperspectives.10476

[24] Lauren Copeland. 2014. Conceptualizing Political Consumerism: How Citizenship Norms Differentiate Boycotting From Buycotting. *Political studies* 62, 1_suppl (2014), 172–186.

[25] Dharma Dailey and Kate Starbird. 2014. Visible skepticism: Community vetting after Hurricane Irene.. In *ISCRAM*.

[26] Emanuela Dalmasso, Adele Del Sordi, Marlies Glasius, Nicole Hirt, Marcus Michaelsen, Abdulkader S. Mohammad, and Dana Moss. 2018. Intervention: Extraterritorial Authoritarian Power. *Political Geography* 64 (May 2018), 95–104. doi:10.1016/j.polgeo.2017.07.003

[27] Rueben Dass and Jasminder Singh. 2023. Pathways to the Caliphate: Mapping Malaysian Foreign Fighter Networks in Iraq and Syria from 2012-2019. *Terrorism and Political Violence* 35, 7 (2023), 1502–1535.

[28] Jade Jiewen Deng and Jason Pridmore. 2024. Digital Dis/connection as everyday boundary work among Hong Kong bn(o) migrants in the UK. *Media and Communication* 12 (Oct 2024). doi:10.17645/mac.8573

[29] Linh Dich. 2016. Community Enclaves and Public Imaginaries: Formations of Asian American Online Identities. *Computers and Composition* 40 (2016), 87–102.

[30] Jill P Dimond, Michaelanne Dye, Daphne LaRose, and Amy S Bruckman. 2013. Hollaback! The role of storytelling online in a social movement organization. In *Proceedings of the 2013 conference on Computer supported cooperative work*. 477–490.

[31] Mary Douglas and Aaron Wildavsky. 1983. *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers*. Univ of California Press.

[32] Jennifer Faull. 2018. L'Oreal Is Doing 'Background Checks' as Part of a New Influencer Vetting Process. https://www.thedrum.com/news/2018/09/13/l-oreal-doing-background-checks-part-new-influencer-vetting-process

[33] Sarah Florini. 2015. The podcast "Chitlin'Circuit": Black Podcasters, Alternative Media, and Audio Enclaves. *Journal of Radio & Audio Media* 22, 2 (2015), 209–219.

[34] Brian CH Fong. 2022. Diaspora Formation and Mobilisation: The Emerging Hong Kong Diaspora in the Anti-Extradition Bill Movement. *Nations and Nationalism* 28, 3 (2022), 1061–1079. doi:10.1111/nana.12804

[35] Eric Fong, Jenny X Li, and Carew CS Chan. 2018. Mainland migrants in Hong Kong. In *Routledge handbook of contemporary Hong Kong*. Routledge, 275–289.

[36] Sarah Fox, Rachel Rose Ulgado, and Daniela Rosner. 2015. Hacking Culture, Not Devices: Access and Recognition in Feminist Hackerspaces. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Vancouver, BC, Canada) *(CSCW '15)*. Association for Computing Machinery, New York, NY, USA, 56–68. doi:10.1145/2675133.2675223

[37] Saipira Furstenberg, Edward Lemon, and John Heathershaw. 2021. Spatialising State Practices Through Transnational Repression. *European Journal of International Security* 6, 3 (2021), 358–378.

[38] Sucheta Ghoshal and Amy Bruckman. 2019. The Role of Social Computing Technologies in Grassroots Movement Building. *ACM Transactions on Computer-Human Interaction (TOCHI)* 26, 3 (2019), 1–36.

[39] Sucheta Ghoshal, Andrea Grimes Parker, Christopher A. Le Dantec, Carl Disalvo, Lilly Irani, and Amy Bruckman. 2019. Design and the Politics of Collaboration: A Grassroots Perspective. *Companion Publication of the 2019 Conference on Computer Supported Cooperative Work and Social Computing* (Nov 2019), 468–473. doi:10.1145/3311957.3359438

[40] Anthony Giddens. 1999. Risk and responsibility. *The Modern Law Review* 62 (1999), 1.

[41] Mark J Goodman. 2007. Diaspora, Ethnicity and Problems of Identity. In *Muslim Diaspora*. Routledge, 80–93.

[42] Yana Gorokhovskaia, Nate Schenkkan, and Grady Vaughan. 2023. Still Not Safe: Transnational Repression in 2022. *Freedom House Washington, DC Accessed August* 30, 2023 (2023), 2023–04.

[43] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a low profile? Technology, risk and privacy among undocumented immigrants. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–15.

[44] Paridhi Gupta, Adrian Petterson, Divyani Motla, and Priyank Chandra. 2022. Ladange, Adange, Jeetange: The Farmers' Movement and Its Virtual Spaces. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (Nov 2022), 1–34. doi:10.1145/3555547

[45] Megan K Halpern, Ingrid Erickson, Laura Forlano, and Geri K Gay. 2013. Designing Collaboration: Comparing Cases Exploring Cultural Probes as Boundary-Negotiating Objects. In *Proceedings of the 2013 conference on Computer supported cooperative work*. 1093–1102.

[46] Monique Hennink and Bonnie N Kaiser. 2022. Sample Sizes for Saturation in Qualitative Research: A Systematic Review of Empirical Tests. *Social Science & Medicine* 292 (2022), 114523.

[47] Ming-Sho Ho. 2024. Hongkongers' International Front: Diaspora Activism During and After the 2019 Anti-Extradition Protest. *Journal of Contemporary Asia* 54, 2 (March 2024), 238–259. doi:10.1080/00472336.2023.2168208

[48] Benjamin Garcia Holgado and Raúl Sánchez Urribarri. 2024. The Dark Side of Legalism: Abuse of the Law and Democratic Erosion in Argentina, Ecuador, and Venezuela. *American Behavioral Scientist* 68, 12 (Nov. 2024), 1578–1596. doi:10.1177/00027642241268332

[49] Amelia Hoover Green. 2016. The commander's dilemma: Creating and controlling armed group violence. *Journal of Peace Research* 53, 5 (2016), 619–632.

[50] Joey Chiao-Yin Hsiao, Sylvia Darling, and Tawanna R Dillahunt. 2023. How Recent Migrants Develop Trust Through Community Commerce: The Emergence of Sociotechnical Adaptation. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW1 (2023), 1–24.

[51] Heli Ikonen, Netta Iivari, and Henrik Hedberg. 2010. Controlling the Use of Collaboration Tools in Open Source Software Development. In *Proceedings of the 6th Nordic Conference on Human-Computer Interaction: Extending Boundaries*. 236–245.

[52] Lilly C Irani and M Six Silberman. 2013. Turkopticon: Interrupting worker invisibility in amazon mechanical turk. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 611–620.

[53] Yong Ming Kow, Yubo Kou, Bryan Semaan, and Waikuen Cheng. 2016. Mediating the Undercurrents: Using Social Media to Sustain a Social Movement. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. Association for Computing Machinery, New York, NY, USA, 3883–3894. doi:10.1145/2858036.2858186

[54] Yong Ming Kow, Bonnie Nardi, and Wai Kuen Cheng. 2020. Be Water: Technologies in the Leaderless Anti-ELAB Movement in Hong Kong. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu HI USA, 1–12. doi:10.1145/3313831.3376634

[55] RE Kraut. 2012. *Building Successful Online Communities: Evidence-based Social Design*. MIT Press.

[56] Joseph Kwaka. 2011. Vetting and Social Audit of Leaders. *Challenging the Rulers: A Leadership Model for Good Governance* (2011), 235.

[57] Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. 2011. We're in It Together: Interpersonal Management of Disclosure in Social Network Services. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 3217–3226.

[58] Ashley Lee. 2018. Invisible networked publics and hidden contention: Youth activism and social media tactics under repression. *New media & society* 20, 11 (2018), 4095–4115.

[59] Ching Kwan Lee and Ming Sing (Eds.). 2019. *Take back our future: an eventful sociology of the Hong Kong Umbrella Movement*. ILR Press, an imprint of Cornell University Press, Ithaca [New York].

[60] Charlotte P Lee. 2005. Between Chaos and Routine: Boundary Negotiating Artifacts in Collaboration. In *ECSCW 2005: Proceedings of the Ninth European Conference on Computer-Supported Cooperative Work, 18–22 September 2005, Paris, France*. Springer, 387–406.

[61] Charlotte P Lee. 2007. Boundary Negotiating Artifacts: Unbinding the Routine of Boundary Objects and Embracing Chaos in Collaborative Work. *Computer Supported Cooperative Work (CSCW)* 16 (2007), 307–339.

[62] Francis L. F. Lee. 2023. Proactive Internationalization and Diaspora Mobilization in a Networked Movement: The Case of Hong Kong's Anti-Extradition Bill Protests. *Social Movement Studies* 22, 2 (March 2023), 232–249. doi:10.1080/14742837.2022.2031957

[63] Francis L F Lee and Chun Hong Tse. 2024. The Critical Online Diasporic Infosphere and Counter-Public Sustenance in an Autocratizing Society. *Inf. Commun. Soc.* (Nov. 2024), 1–18.

[64] Peter S. Li. 2005. The Rise and Fall of Chinese Immigration to Canada: Newcomers from Hong Kong Special Administrative Region of China[1] and Mainland China, 1980–2000[2]. *International Migration* 43, 3 (Aug. 2005), 9–34. doi:10.1111/j.1468-2435.2005.00324.x

[65] Kelley Loper. 2010. Human Rights, Non-Refoulement and the Protection of Refugees in Hong Kong. *International Journal of Refugee Law* 22, 3 (2010), 404–439.

[66] Deborah Lupton. 2024. *Risk*. Routledge.

[67] Alex Marland. 2021. Vetting of Election Candidates by Political Parties: Centralization of Candidate Selection in Canada. *American Review of Canadian Studies* 51, 4 (2021), 573–591.

[68] Alex Marland and Brooks DeCillia. 2020. Reputation and Brand Management by Political Parties: Party Vetting of Election Candidates in Canada. *Journal of Nonprofit & Public Sector Marketing* 32, 4 (2020), 342–363.

[69] Roger C Mayer, James H Davis, and F David Schoorman. 1995. An Integrative Model of Organizational Trust. *Academy of management review* 20, 3 (1995), 709–734.

[70] Marcus Michaelsen and Johannes Thumfart. 2023. Drawing a Line: Digital Transnational Repression Against Political Exiles and Host State Sovereignty. *European Journal of International Security* 8, 2 (2023), 151–171.

[71] Blake W Mobley and Carl Anthony Wege. 2021. Counterintelligence vetting techniques compared across multiple domains. *International Journal of Intelligence and CounterIntelligence* 34, 4 (2021), 663–693.

[72] Luiza Monetti. 2024. Wolves in Sheep's Clothing: The Autocratic Subversion of Brazil's Fourth Estate. *American Behavioral Scientist* 68, 12 (Nov. 2024), 1636–1654. doi:10.1177/00027642241268346

[73] Dana M. Moss. 2018. The ties that bind: Internet communication technologies, networked authoritarianism, and 'voice' in the Syrian diaspora. *Globalizations* 15, 2 (Feb. 2018), 265–282. doi:10.1080/14747731.2016.1263079

[74] Dana M. Moss, Marcus Michaelsen, and Gillian Kennedy. 2022. Going after the family: Transnational repression and the proxy punishment of Middle Eastern diasporas. *Global Networks* 22, 4 (Oct. 2022), 735–751. doi:10.1111/glob.12372

[75] Helen Nissenbaum. 2004. Privacy as Contextual Integrity. *Washington Law Review* 79 (2004), 119.

[76] Helen Nissenbaum. 2011. A Contextual Approach to Privacy Online. *Daedalus* 140, 4 (2011), 32–48.

[77] Political Vetting of Community Work Working Group et al. 1990. Political Vetting of Community Work in Northern Ireland. (1990).

[78] Thomas O'Brien. 2015. Social control and trust in the New Zealand environmental movement. *Journal of Sociology* 51, 4 (2015), 785–798.

[79] Leysia Palen and Paul Dourish. 2003. Unpacking" privacy" for a networked world. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. 129–136.

[80] Adrian Petterson, Ashique Ali Thuppilikkat, Paridhi Gupta, Shamika Klassen, Margaret C Jack, Jun Liu, and Priyank Chandra. 2023. Supporting Social Movements Through HCI and Design. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–5.

[81] Sandra Ponzanesi. 2020. Digital diasporas: Postcoloniality, media and affect. *Interventions* 22, 8 (2020), 977–993.

[82] Lubna Razaq and Sucheta Ghoshal. 2025. The Role of ICTs in the Maintenance and Reproduction of Digital Border Assemblages. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. 1–17.

[83] Jamie Rowen. 2012. Mobilizing truth: Agenda setting in a transnational social movement. *Law & Social Inquiry* 37, 3 (2012), 686–718.

[84] Nate Schenkkan, Isabel Linzer, Saipira Furstenberg, and John Heathershaw. 2020. Perspectives on "Everyday" Transnational Repression in an Age of Globalization.

[85] Wong Siu-Lun. 1992. Emigration and stability in Hong Kong. *Asian Survey* 32, 10 (1992), 918–933.

[86] Paul Slovic. 1987. Perception of Risk. *Science* 236, 4799 (1987), 280–285.

[87] Paul Slovic, Ellen Peters, Melissa L Finucane, and Donald G MacGregor. 2005. Affect, risk, and decision making. *Health psychology* 24, 4S (2005), S35.

[88] Frederic Stutzman and Woodrow Hartzog. 2012. Boundary regulation in social media. In *Proceedings of the ACM 2012 conference on computer supported cooperative work*. 769–778.

[89] Fred Stutzman and Jacob Kramer-Duffield. 2010. Friends only: examining a privacy-enhancing behavior in facebook. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 1553–1562.

[90] Nicole Tang and Priyank Chandra. 2022. Community, Culture, and Capital: Exploring the Financial Practices of Older Hong Kong Immigrants. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts*. 1–6.

[91] The Government of the Hong Kong Special Administrative Region. 2021. Mid-year population for 2021. Press Release. https://www.info.gov.hk/gia/general/202108/12/P2021081200387.htm

[92] The Hong Kong Institute of Asia-Pacific Studies. 2024. Survey findings on views about emigration from Hong Kong released by the Hong Kong Institute of Asia-Pacific Studies at CUHK. *The Chinese University of Hong Kong* (Nov 2024). https://www.cpr.cuhk.edu.hk/en/press/survey-findings-on-views-about-emigration-from-hong-kong-released-by-the-hong-kong-institute-of-asia-pacific-studies-at-cuhk-4/#:~:text=About%20three%2Dfifths%20of%20the,%25)%20had%20a%20positive%20outlook

[93] Ashique Ali Thuppilikkat, Janna Akimova, and Priyank Chandra. 2025. Dissent, Distance, Dilemmas: ICTs and the Belarusian Diasporic Social Movement Community. *Proceedings of the ACM on Human-Computer Interaction* 9, 7 (2025), 1–31. doi:10.1145/3757469

[94] Kin-long Tong. 2025. A Decentralized, Community-Led Library for Diasporic Communities: The Case of the Hong Kong BookShare in the UK. *Journal of Librarianship and Information Science* (Apr 2025). doi:10.1177/09610006251334403

[95] Özgün E Topak. 2019. The Authoritarian Surveillant Assemblage: Authoritarian State Surveillance in Turkey. *Security Dialogue* 50, 5 (2019), 454–472.

[96] Gerasimos Tsourapas. 2021. Global Autocracies: Strategies of Transnational Repression, Legitimation, and Co-optation in World Politics. *International Studies Review* 23, 3 (2021), 616–644.

[97] Rajesh Veeraraghavan. 2013. Dealing With the Digital Panopticon: The Use and Subversion of ICT in an Indian Bureaucracy. In *Proceedings of the Sixth International Conference on Information and Communication Technologies and Development: Full Papers-Volume 1*. 248–255.

[98] Yaniv Voller. 2023. Militias as a Tool for Encouraging Ethnic Defection: Evidence From Iraq and Sudan. *Terrorism and political violence* 35, 1 (2023), 65–82.

[99] Mariëlle Wijermars and Tetyana Lokot. 2022. Is Telegram a "Harbinger of Freedom"? The Performance, Practices, and Perception of Platforms as Political Actors in Authoritarian States. *Post-Soviet Affairs* 38, 1-2 (2022), 125–145.

[100] Kennedy Chi-Pan Wong. 2024. Sowing Hate, Cultivating Loyalists: Mobilizing Repressive Nationalist Diasporas for Transnational Repression by the People's Republic of China Regime. *American Behavioral Scientist* 68, 12 (Nov. 2024), 1655–1678. doi:10.1177/00027642241267931

[101] Volker Wulf, Kaoru Misaki, Meryem Atam, David Randall, and Markus Rohde. 2013. 'On the Ground' in Sidi Bouzid: Investigating Social Media Use During the Tunisian Revolution. In *Proceedings of the 2013 conference on Computer supported cooperative work*. 1409–1418.

[102] Miu Chung Yan, Barbara Lee, Sean Lauer, Tsz Chung Ngai, Frankie Cabahug, and Capri Kong. 2025. Survey Study on Hong Kong Residents Recently Arrived in Canada (Second Wave): Preliminary Report. doi:10.14288/1.0447864

[103] Daisy Yoo, Katie Derthick, Shaghayegh Ghassemian, Jean Hakizimana, Brian Gill, and Batya Friedman. 2016. Multi-Lifespan Design Thinking: Two Methods and a Case Study With the Rwandan Diaspora. In *Proceedings of the 2016 CHI conference on human factors in computing systems*. 4423–4434.

[104] Ben Zefeng Zhang, Oliver L. Haimson, and Michaelanne Thomas. 2022. The Chinese Diaspora and The Attempted WeChat Ban: Platform Precarity, Anticipated Impacts, and Infrastructural Migration. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2, Article 397 (Nov. 2022), 29 pages. doi:10.1145/3555122

[105] Jinman Zhang and Nadia Caidi. 2019. The Sensitive Period, Big Vs, and the Diaspora: A Brief Account of #MeToo in China. In *Proceedings of the 10th International Conference on Social Media and Society*. 224–232.

[106] Lichen Zhen. 2021. Social Coding Platform as Digital Enclave: A Case Study of Protesting "996" on GitHub. *International Journal of Communication* 15 (2021), 19.