

USENIX

THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Resilience Amid Diffused Surveillance During a Political Movement in Bangladesh

Mashiyat Mahjabin Eshita, *BRAC University;* Ishmam Bin Rofi, *Rochester Institute of Technology;* Md. Sabbir Ahmed, *BRAC University;* Dipto Das, *University of Toronto;* Md. Golam Rabiul Alam, *BRAC University;* Jannatun Noor, *C2SG Research Group, United International University;* Syed Ishtiaque Ahmed, *University of Toronto;* S M Taiabul Haque, *BRAC University*

https://www.usenix.org/conference/usenixsecurity26/presentation/eshita

This paper is included in the Proceedings of the 35th USENIX Security Symposium.

August 12–14, 2026 • Baltimore, MD, USA

ISBN 978-1-939133-58-8

Open access to the Proceedings of the 35th USENIX Security Symposium is sponsored by



جامعة الملك عبدالله للعلوم والتقنية

King Abdullah University of Science and Technology

ARTIFACT EVALUATED
USENIX
AVAILABLE

Resilience Amid Diffused Surveillance During a Political Movement in Bangladesh

Mashiyat Mahjabin Eshita[1,*] Ishmam Bin Rofi[2,*] Md. Sabbir Ahmed[1,*] Dipto Das[3]
Md. Golam Rabiul Alam[1] Jannatun Noor[4] Syed Ishtiaque Ahmed[3] S M Taiabul Haque[1]
[1]*BRAC University, Bangladesh* [2]*Rochester Institute of Technology, USA*
[3]*University of Toronto, Canada* [4]*C2SG Research Group, United International University, Bangladesh*

Abstract

In July 2024, Bangladesh witnessed a historic, student-led uprising where social media became both a tool of mobilization and a site of repression. While surveillance is often framed through Bentham's vertical Panopticon model, our study extends the discourse on lateral surveillance. Drawing on 23 interviews with protesters, activists, and digital organizers, we examine how lateral surveillance operates within a political movement in Bangladesh, where discipline is enacted not only by the state but also through peers, kin, and intimate social ties. Participants described living under constant fear while also developing creative strategies of resilience, from improvised encrypted systems and panic deletions to cultural tactics like satire and hidden speech. We contribute to security and privacy literature on activism by highlighting the need for designs that strengthen safety, anonymity, and collective resilience in fragile and repressive contexts.

1 Introduction

On 5 August 2024, Bangladesh witnessed the resignation of its long-serving prime minister following weeks of mass student-led protests. Sparked by the reinstatement of the quota system for government jobs, the movement quickly escalated into one of the largest youth uprisings in the country's history [110]. Social media became the frontline of mobilization, where people shared memes, news, and updates [62, 108], however, it was also the key site of repression, where activists faced censorship, surveillance, and harassment [22, 119]. These dual dynamics turned platforms into both enablers of collective voice and infrastructures of fear.

Globally, scholars have shown how digital infrastructures simultaneously empower and endanger activism [92]. In many countries, infrastructures often amplify collective action: the Black Lives Matter movement leveraged livestreams and hashtags to draw visibility to racial injustice, coordinate protests across multiple cities, and sustain public attention over months [35, 79]. Similarly, protesters in Hong Kong's Anti-Extradition Law Amendment Bill (Anti-ELAB) movement relied on encrypted apps to coordinate securely and evade police surveillance, illustrating how infrastructures can enable both scale and secrecy under pressure [66]. These cases highlight the enabling potential of platforms for organizing, broadcasting, and sustaining dissent. In the Global South, however, infrastructures that enable resistance are also fragile and easily weaponized. During Myanmar's Spring Revolution, repeated internet shutdowns slowed communication and fractured organizing capacity, leaving activists isolated from each other and the global public sphere [48, 100].

Besides, in Iran's "Woman, Life, Freedom" uprising, activists navigated both digital censorship and lethal repression, demonstrating how online risks often escalate directly into offline violence, creating a constant atmosphere of fear [88, 97]. These cases illustrate how infrastructures in the Global South collapse the boundary between digital platforms and everyday survival. Bangladesh's July 2024 uprising adds to this landscape, demonstrating how infrastructures can both accelerate mobilization and fragment it through targeted surveillance and blackouts.

Surveillance is traditionally framed through Bentham's Panopticon (centralized visibility) [19, 104] and Foucault's notion of self-discipline under the possibility of being watched [123]. While influential, these perspectives emphasize vertical, top-down control [105]. The second generation of surveillance scholarship gradually deviates from panopticism to conceptualize surveillance as a decentralized, networked ecosystem [44]. The post-panoptic notion of "surveillant assemblage" represents a mesh of different modern technologies (e.g., social media, CCTV, etc.) working together to monitor and track individuals [37]. Moreover, lateral surveillance – the act of ordinary individuals monitoring one another, often using digital tools – further advances the understanding of surveillance in today's world [9, 10]. Our study joins this modern discourse on surveillance by showing that during Bangladesh's uprising, surveillance also operated *laterally*, enacted by peers, family members, and neighbors alongside

*These authors contributed equally to this work.

state monitoring. In this sense, surveillance was not contained in a tower but diffused across infrastructures, laws, and intimate social ties. In many ways, this diffusion pattern is contextually different from the concept of lateral surveillance in the existing literature [9, 10], and we extend the discourse on lateral surveillance by focusing on the recent political movement in Bangladesh.

In this paper, we draw on 23 in-depth interviews with protesters, activists, and digital organizers in Bangladesh to understand how surveillance and censorship were experienced during the movement, and how participants responded with resilience. Our study highlights two dynamics: first, how surveillance extended laterally into families, peers, and social ties, blurring the boundary between state power and citizen enforcement; and second, how participants developed creative strategies to sustain communication and resist censorship under extreme risk. From this, we ask:

- *RQ1.* How did participants experience surveillance and censorship during the July 2024 Quota Reform Movement in Bangladesh, and in what ways did these practices extend beyond the state to involve peers, family members, and social ties?

- *RQ2.* What strategies of digital resilience and resistance did protesters develop to navigate censorship, internet shutdowns, and fear?

By addressing these questions, we make a threefold contribution to security and privacy literature on activism and political movements. First, we identify a new threat model where intimate ties relay state pressure into the home during a movement. Second, we describe a catalog of novel, in-situ defensive practices during a nationwide crackdown. Third, we propose design directions for coercion-based threats that Global North protections do not address. Taken together, our work joins the growing body of security and privacy scholarship on protecting the digital rights of at-risk protesters in different parts of the world [25, 48].

2 Background and Related Work

In this section, we situate the July 2024 Revolution within the broader context of works on social movements and digital infrastructures. Rather than treating technologies as neutral tools, we follow scholarship that frames infrastructures as structural actors that can amplify, suppress, or redirect resistance [54, 55].

2.1 Bangladesh's July 2024 Revolution

The July 2024 Revolution in Bangladesh unfolded through sparks, accelerations, frictions, and surges. It began on 5 June 2024 when the High Court reinstated the freedom-fighter quota, sparking protests at Dhaka University and other campuses that drew national attention through television [3]. Momentum accelerated on 14 July as private university students joined and Facebook amplified memes, satire, and livestreams of police brutality despite repression [14]. On 15 July, attacks by regime-aligned groups and security forces forced protests into the streets [58]. Friction emerged on 18 July with a sweeping nationwide blackout that simultaneously cut broadband, mobile data, and all major social media. Crucially, this was phased, not a single disruption: broadband returned selectively on 23–24 July, mobile internet on 28 July, and social media only on 31 July. By 4 August, the surge peaked as hubs like Shahbagh were paralyzed amid the deadliest clashes of the uprising [95]. On 5 August, the regime collapsed, with senior figures fleeing abroad [120].

Digital Momentum

The revolution also demonstrates how infrastructures shaped the pace and scope of collective action [78]. Earlier uprisings in Bangladesh leaned on print and cultural media such as songs, plays, graffiti, puppetry, and satire [40], but in 2024, digital platforms transformed mobilization into a rapid cascade. This digital orientation reflects broader media habits among Bangladeshi youth, over 70% of whom identify social media as their primary source of news [106]. Therefore, what began at Dhaka University quickly surged once it reached Facebook, the country's dominant platform [14]. Memes, satire, crackdown footage, and testimonies circulated millions of times, drawing national and international attention [62]. Figure 1 provides a timeline of how these infrastructural dynamics unfolded.

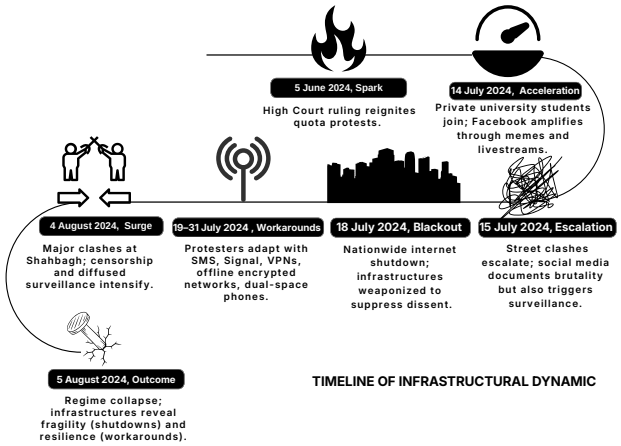

Figure 1: Timeline of the July 2024 Revolution in Bangladesh, illustrating the cascade from initial spark to outcome.

2.2 Momentum Across Global Contexts

Social movements have transformed dramatically over time, and social media enables them to gain momentum faster than ever [27]. On the one hand, robust connectivity and device access allow movements to leverage visibility tools (e.g., hashtags, viral campaigns) [63]. On the other hand, these same infrastructures expose activists to algorithmic suppression, harassment, and surveillance [41]. In particular, if local infrastructures are fragile and contested, weaker access and strong political control make digital systems prone to shutdowns, censorship, and direct weaponization by authorities.

Recent scholarship demonstrates that governance extends beyond direct coercion. It can function as "social control" through prestige and reward systems [47], and can also operate when the state encourages citizens to denounce one another [20]. These dynamics align with Chriss's concept of "informal social control," where the state harnesses daily interactions to transform personal disputes into a mechanism for broader order [33]. Such control is most effective when overt authority is less visible, as individuals internalize powerlessness and self-regulate themselves [72]. In China, this logic appears in state–private surveillance collaborations that serve national goals of security and social stability [32]. However, evidence from high-violence contexts shows that governance beyond direct coercion depends on perceived legitimacy: fear and consent often coexist, complicating the translation of authority into voluntary compliance [61].

The digital infrastructures often act as accelerators of visibility and coordination. Occupy Wall Street used social media and livestreaming to broadcast the movement and constitute itself as a collective actor [2]. Protesters in Hong Kong's Anti-Extradition Law Amendment Bill (Anti-ELAB) movement utilized encrypted platforms like Telegram and WhatsApp for coordination, while livestreaming on Facebook and YouTube to increase visibility [6]. Research shows that expressive uses of social media, such as sharing political content or connecting with activists, are strong predictors of both attitudinal support and street participation, as seen in the Hong Kong Umbrella Movement [69].

The Arab Spring revealed that while structural grievances such as unemployment and corruption were decisive, digital tools amplified dissent and accelerated coordination once uprisings began [73]. Similar patterns are evident in Bangladesh and beyond: platforms help sustain protest during quiet periods, speed up coordination when action begins, and diffuse discontent across networks [122]. Social media thus operates less as a neutral tool and more as a velocity engine, reshaping the rhythm of collective action. Besides, the #MeToo movement turned personal testimonies into collective accountability [31]. Black Lives Matter (BLM) – after George Floyd's killing – exemplifies these dynamics: livestreamed videos shaped debates on accountability [16], while the hashtag #BlackLivesMatter was used 47.8 million times in less than two weeks, turning online visibility into global solidarity [8]. As many attendees were novice protesters, the security and privacy advice given to them has been investigated extensively as well [25].

In many contexts, the digital infrastructures reveal fragility and friction. Myanmar's Spring Revolution was slowed by repeated internet shutdowns, forcing activists into ICT workarounds [48]. These internet shutdowns affect both local and diaspora communities, resulting in cross-border human rights violations [115]. In Sri Lanka, the #GoHomeGota2022 hashtag accelerated dissent and contributed to leadership change [96]. The Arab Spring illustrated how platforms could ignite uprisings but also entrap dissent under authoritarian surveillance [7]. Recent scholarship further points to the expanding role of military-driven digital surveillance in semi-authoritarian regimes [87]. Iran's 2022–2023 "Woman, Life, Freedom" uprising showed how activists used digital counter-appropriation despite lethal repression [91]. Bangladesh's 2024 Gen Z-led uprising amplified student protests into a nationwide mobilization [14]. In Indonesia, protests over parliamentary allowances escalated into violence, with the government labeling unrest as "terrorism" and deploying the military [113]. During the recent pro-democracy movement in Hong Kong, doxxing – the act of deliberately seeking and publishing targets' personal information without consent – has emerged as a widespread practice [68]. A recent study with Canadian police officers reveals that not only the protesters but also the law enforcement officials are subjected to doxxing as a form of harassment [57].

Our work is informed by these studies, which reveal that while digital infrastructures often act as stable accelerators of visibility, they could also become fragile engines, vulnerable to shutdowns, censorship, and capture. Against these backdrops, it seems reasonable to deeply investigate the technology-mediated July 2024 uprising in Bangladesh, which displays accelerators (memes, livestreams) alongside frictions (blackouts, censorship).

2.3 Surveillance, Censorship, and Local Resistance

2.3.1 Freedom of Expression and Resistance

States adapt quickly to digital protest dynamics, deploying shutdowns, censorship, throttling, surveillance, and disinformation to impose a drag [41]. When states attempt to suppress dissent, activists improvise technically and culturally. VPNs, encrypted apps, and burner accounts coexist with memes, satire, and coded speech [86, 94, 124]. Beyond explicitly technological responses, research also documents non-digital counter-surveillance practices, including low-tech defensive tactics [36] and embodied, everyday surveillance from below [17].

Activists across contexts demand safer, more transparent

platforms [75, 99], yet algorithmic opacity, hate speech, and misinformation weaken their ability to organize support [74]. In Bangladesh, repressive laws such as the ICT and Digital Security Acts (DSA) fostered fear and self-censorship, yet also galvanized youth to adopt tactics grounded in anonymity, humor, and strategic ambiguity [107, 114].

2.3.2 Surveillance as Panoptic Discipline → Networked Control → Lateral Monitoring

The scholarship on surveillance can be broadly categorized into three phases [44]. While the first phase mostly describes physical and spatial attributes, characterized by Bentham's panopticism and Foucault's notion of self-discipline [19, 43, 123], the second phase proposes infrastructural and networked theories of surveillance that rely on digital technologies. This post-panoptic surveillance literature is rooted in Deleuze's seminal work [37], which argues a shift from Foucault's "disciplinary societies" to "societies of control" that track individuals via data. Haggerty and Ericson draw inspiration from this idea to propose the concept of "surveillant assemblage" that views surveillance as a convergence of formerly discrete monitoring and tracking mechanisms, resulting in a "data double" of an individual [49]. Zuboff proposes a different framework based on surveillance capitalism that is driven by profit-making incentives [125]. Our work is situated within the third phase of surveillance literature, which is characterized not so much by novel theories, but rather by adoption of prior theories in specific contexts [44]. In particular, we adopt Andrejevic's concept of lateral surveillance in the context of July 2024 Movement in Bangladesh [9, 10].

Lateral surveillance highlights how peer monitoring develops among social equals and within everyday relations, such as friends and family [9, 10]. The concept of lateral or horizontal surveillance has been investigated in various contexts, including corporate environments [18], factories [45], hospitals [89], monasteries [64], concentration camps [70], and prisons [59]. Still, this framework offers only limited insight into the pressures circulating through tightly bound intimate networks, where compliance emerges from obligation, dependency, and shared histories [26, 71, 81, 93]. As the existing scholarship tends to focus on vertical oversight by authorities or broad peer-level monitoring, the microdynamics of surveillance embedded in intimate relations remain underexamined [21, 118].

Andrejevic points out that monitoring now goes hand-in-hand with interactive technology, enabling continuous monitoring of individuals and storage of this information in machine-readable formats [11, 121]. This marks a shift from the disciplinary model, where traditional surveillance relies on awareness to enforce behavior, automated models capture "undisciplined activity" to categorize and anticipate actions [12]. Scott adds an administrative layer, explaining how states make populations legible through registries, IDs, and bureaucratic tools [103]. Such infrastructures generate archives and traces for later scrutiny of the watchers [83, 109]. Together, these perspectives illustrate why digital repression often relies less on constant policing than on uncertainty, self-censorship, and expanding systems that classify and document citizens.

However, these institutional frameworks only capture part of the picture. While Foucault's analysis is rooted in European institutions, it pays less attention to how surveillance operates in contexts shaped by colonial legacies and ongoing structural inequalities [111, 112]. In many Global South settings, power is shaped by different histories [77], uneven infrastructures [80], and strongly collective social arrangements [82]. Monitoring is often facilitated by dense networks of kinship, obligation, and shared responsibility [39], as well as shared digital practices that make personal information continuously visible to co-users and family members [4, 67, 85]. This contrasts with patterns more common in Global North contexts, where social life tends to be more individualistic [117], and where surveillance is imagined primarily as an institutional or technological process rather than a relational one [76]. However, instances of social surveillance were recorded in Australia during the COVID-19 pandemic [13]. Despite these findings, a significant gap remains. Therefore, recognizing this gap helps adjust classic theories so they better reflect the intimate, historically layered forms of surveillance shaping everyday activism in places like Bangladesh.

3 Methodology

In this study, we focused on how social media became a site of surveillance and censorship during the July 2024 protest in Bangladesh, and how participants developed creative strategies of digital resilience to navigate blackouts, monitoring, and risks embedded in their everyday social ties. We conducted our study over a six-month period, from February 2025 to July 2025. A total of 23 participants (14 males and 9 females), aged between 18 and 55 years, were recruited for the study. Our participants came from various professions, including students, university faculty members, social media page administrators, sociologists, and anthropologists. For the student participants, we recruited individuals from diverse institutions in Dhaka based on their involvement in the uprising. The demographic information of the participants is provided in Appendix B.

3.1 Participant Recruitment and Interview Procedure

Given the politically sensitive and context-specific nature of the July 2024 Movement, we adopted a *purposive sampling* strategy [28, 42, 116], supplemented by convenience and snowball approaches. We began recruitment with friends and colleagues who were vocal and active on social media during the protests, then expanded outreach through social media

platforms. To widen participation, we circulated a Google Form describing the study, which allowed interested individuals to sign up. When recruiting the participants, we also considered the relevance of their experiences to our research focus on social media, surveillance, and resilience. We recruited and interviewed participants until our data reached thematic saturation, where no substantively new themes were emerging from additional interviews.

For data collection, we conducted one group discussion with two participants (15 and 16) who had co-developed a platform during the protest and preferred to be interviewed together. All other interviews were conducted individually, either online (via Google Meet, WhatsApp, or traditional phone calls) or offline at the university campus of one of the authors, depending on participants' availability and preference. Three of the authors were involved in conducting the interviews. All interviews were conducted in a semi-structured format. The interview guide is provided as supplementary material.

All interviews were conducted in Bengali, participants' primary language. We obtained both verbal and written consent, clearly explaining the study's purpose and ensuring anonymity. For online interviews, consent was collected through a Google Form. Participants were informed that they could withdraw at any point, skip questions, and that their responses would remain confidential. All participants agreed to be recorded, with recordings stored securely on a university computer accessible only to the authors. We also clarified who would have access to transcripts and assured that all data would be permanently deleted after study completion.

3.2 Data Analysis

For data analysis, three authors who are native Bengali speakers manually transcribed and translated the interviews without the use of automated tools. This approach enabled careful interpretation of local expressions, tone, and politically situated meaning. Analysis began concurrently with data collection, following an iterative and grounded process that informed subsequent interviews [46]. We conducted inductive thematic analysis [24, 34], allowing analytic categories to emerge from participants' accounts rather than relying on predefined themes.

Three members of the research team independently coded each transcript using open coding. Coding agreement was established through a series of regular team meetings in which authors compared interpretations, discussed differences, and refined analytic decisions through collective deliberation. Rather than enforcing a fixed or predefined codebook, the coding schema evolved throughout analysis and was documented internally through shared analytic notes to support consistency across transcripts.

Due to the highly sensitive and politically charged nature of the data, and explicit commitments made to participants regarding confidentiality and non-disclosure, analytic artifacts such as detailed coding schemas or transcripts cannot be publicly released. After completing coding, the research team collaboratively clustered related codes into higher-level themes, which are reported in the following section.

4 Findings

Our findings reveal how surveillance – both state and non-state – took place during the July 2024 Quota Reform Movement in Bangladesh. The state actors broadly fall into two categories: (1) law enforcement agencies, including police, immigration inspectors, and prison administrators, (2) cyber administration authorities, particularly government agencies responsible for Internet blackout and deep packet inspection. The non-state actors include private internet service providers and pro-regime wings, as well as kin members who impose surveillance out of fear and safety concerns.

We begin with two extended vignettes that capture the lived experiences of surveillance and resilience, then turn to broader patterns across participants' accounts.

Vignette 1: Living Under the Shadow of Repressive Laws

Surveillance in Bangladesh is sustained not only by technological systems but by an atmosphere of fear and legality that infiltrates everyday life.

> "Take the 2018 movement, for example – the first revolt came from kids whose friends had been killed. From then on, the state began tracking people who liked or shared certain posts. Those people were detained or attacked. [...] Bangladesh's political battlefield existed mostly inside Facebook. You couldn't speak on mainstream media. You couldn't organize a gathering without getting beaten up. [...] One law after another came to suppress any critical voice. And the worst part? Citizens were turned against each other. How? Look at how many cases were filed under ICT laws—people using the law to frame one another. These laws became a tool for mutual harassment between citizens. [...] In 2018, the Digital Security Act arrived, while the earlier ICT laws were still active. [...] Even between 2023 and 2024, many of us protested against the DSA. What happened? The law got rebranded, not repealed. [...] And even now, there's no public discourse on the surveillance tools the government uses." [Participant 6]

This account illustrates how ICT and DSA laws[1] enabled citizens to report, target, or intimidate one another, blurring the boundary between state-enforced control and peer-

[1] For the details of the relevant legal provisions, see Appendix A.

enforced policing. As the wording of the act shows, it has been intentionally made broad, and words such as "obscene", "deteriorate law and order", and "prejudice the image" are open to subjective interpretations, which could be used by pro-regime individuals and entities to initiate legal action and suppress the protesters. These non-transparent legal mechanisms and shifting regulations create persistent uncertainty, compelling activists to navigate scrutiny from both authorities and their own social circles.

Vignette 2: Crafting Resistance Through Offline Networks

Facing a nationwide internet blackout and pervasive surveillance, some participants turned to technical improvisation, engineering an offline, encrypted platform to sustain communication.

> "When the internet was off, we first tried to use text messaging via phone network, but we were sure that all our messages were going through DPI[2], which was an open secret in Bangladesh, so we tried to make a platform to chat. [...] We knew that all the routers in Bangladesh are connected through BDIX[3], so if we made a platform on our personal desktop and made the IP live, everyone could use it. But the problem was safety, so we took some measures. First, we implemented a dual room system. The public room was for general conversation; sensitive discussions were prohibited there. Private chat rooms had their own room ID and password; only people with the credentials could join, and even we, the admins, could not enter without them. Secondly, we made the system anonymous; people could take a pseudonym and start chatting without using their IP address, phone number, or email. [...] We also introduced a panic button — if the chat room was compromised, pressing it would immediately destroy everything. All texts are automatically deleted after a certain period. We also ensured that our messages weren't going through government gateways monitored by DPI, since encrypted packets could trigger them." [Participant 15]

This vignette highlights how activists built their own secure communication systems rather than relying on existing platforms. Their approach embedded features like panic deletion, pseudonymity, and locally hosted networks to avoid state monitoring—demonstrating how surveillance shaped not only what tools they used but how they engineered them.

[2]Deep packet inspection, a method of analyzing internet traffic that can enable monitoring, filtering, or blocking of communications [90].

[3]BDIX refers to Bangladesh Internet Exchange Point.

4.1 Censorship During the Uprising

Our study revealed a surge in social media censorship and a systematic crackdown on online expression during the uprising. Pro-regime forces actively sought to silence dissenting voices, using both intimidation and legal instruments. Participants described how these mechanisms directly disrupted their lives. One participant was arrested by security forces, his phone was confiscated and searched under the accusation that he had been organizing the protests. Without any formal investigation, he was sent to prison. After his release on bail in early August, his phone was never returned to him. His experience reflects a broader pattern across our data: uncertainty about what might be examined, how it might be interpreted, and how it could later be weaponized against them led many activists to adopt heightened caution and self-censorship.

> "I was arrested in the later part of the movement after the blackout. [...] The cybercrime team took our phones. They checked everything—my gallery, personal texts on Messenger, WhatsApp, everything. [...] After checking the texts, they told me, 'So, you are the leader, right?' And then they sent me to prison. I was in prison till the movement ended. My phone was confiscated, and I could not find it yet." [Participant 13]

The participant further shared that censorship continued inside the prison walls. Prisoners were denied regular communication with their families and had little access to outside information. Even the newspapers they received were censored—pages torn out or sections deliberately removed. These practices reveal how censorship extended beyond digital spaces into the realm of incarceration, severing detainees from both personal and national realities. By withholding information and circulating edited newspapers, authorities created a tightly controlled informational vacuum that deepened uncertainty and reinforced fear among prisoners.

> "Inside the prison, we were not allowed to contact our families. [...] The newspapers we were provided were censored; there were pages missing or parts of pages removed. [...] We were totally uninformed and were censored from the information about the period." [Participant 13]

Censorship was not confined to prisons or protest sites; participants who attempted to leave Bangladesh during the blackout also encountered state scrutiny. One participant recounted how, in the final days of the internet shutdown, he tried to travel abroad to protect his freelance work but was stopped at the airport. Immigration officers interrogated him and confiscated his phone for inspection.

> "I was trying to leave Bangladesh on the final days of the blackout [..]. An airport officer called me

to the desk, asked where I studied, and immediately asked for my phone and told me to unlock it. He took the phone and searched everywhere for evidence that was on my phone – my gallery, my personal photos, and everything." [Participant 16]

The censorship and crackdown on social media activists was expanded to residential homes, and also by IP blocking in some cases. One of our participants, who was part of a team that created an end-to-end encrypted platform using a mesh network to communicate during the internet blackout, informed us that he had been totally blacked out by the regime as his IP address was totally blocked by the gateway controllers.

> "After the internet blackout, our chat platform gained massive popularity—we were handling 300+ signups per hour. The IP we used was my home connection. [...] A whistleblower warned us: 'Your IP is being watched; BTRC has ordered a crackdown.' That night, my internet was gone while my friends' and neighbors' connections worked fine. I realized I had been compromised. The authority had shut down my IP, and the platform was also gone. I was terrified, checking from my balcony if someone was coming for me. I couldn't relaunch the platform and had to use a shared IP for the rest of the movement, as I believe I was tracked." [Participant 15]

Beyond IP blocking, we have found that many of our participants had their homes raided by law enforcement agencies during the movement because of their involvement in the movement, both physically and virtually. One of our participants was an admin of a large Facebook page in Bangladesh; his page had more than 50,000 followers, and he was also a moderator of a large Facebook group helping the protesters. He claimed that his house was raided twice during the protest, and he had to live on the rooftop of his house during the protest.

> "I was the admin of a page with massive influence during the movement. [..] During the blackout, two moderators of the groups were arrested, so I was pretty sure they were coming after me. And it happened, law enforcement agencies tried to raid my house twice. On the first day, late at night, they knocked on the main gate of my building and asked if any students lived there. [..] My apartment mate and I hid our laptops under the false roof of our washroom and went to our rooftop. [..] We spent the rest of the blackout days on the rooftop. We were drenched in rain, and we hid ourselves from the drones. The law enforcement agency tried to raid again, but we were luckily saved." [Participant 18]

His account reveals how state surveillance blurred the boundary between the digital and the domestic. The home, typically imagined as a private refuge, became an extension of the protest field, a place of fear and concealment. Acts as simple as hiding a laptop or changing location became strategies of survival in an atmosphere where visibility itself was incriminating. However, this climate of fear extended far beyond prominent activists and social media organizers. Ordinary citizens who had merely expressed support online also faced scrutiny and pressure. One participant shared how her home was raided, prompting her parents to fear further repercussions. Their anxiety led them to monitor their own online behavior, turning familial care into a form of self-policing.

> "My home was raided late at night. [.. ..] I was the only university student in our building; all the others were school-goers. So, of course, I was the target. After this incident, my parents were scared, and they told me to back off and delete everything I posted. But I still posted on social media, I posted and deleted after 1-2 hours, before my parents found out. My father also checked my phone during that time to see if I had posted anything on social media." [Participant 10]

Her experience underscores how censorship and surveillance permeate domestic relationships, reshaping the dynamics of trust and protection within families. Fear circulated as an emotional contagion, compelling individuals to regulate not only their own actions but also those of their loved ones. In this way, state-imposed control was reproduced through intimate spaces, transforming the household into another layer of the surveillance network. The same pattern appeared in the experiences of other participants who were not visibly active online but supported the movement in indirect ways. One participant, who had merely helped students with logistics, discovered that law enforcement agencies had attempted to trace him through university records. His account reveals how surveillance extended beyond social media into institutional infrastructures, where digital traces and administrative data could be mobilized to locate and intimidate individuals.

> "So, I provided logistics to the protesters during the movement. [..] I was not active on social media or anywhere. Now, during the blackout, as far as my knowledge goes, law enforcement agencies tried to find me. Fortunately, my home address changed a few months ago from the one provided on my university database. So, they searched my previous apartment. I guess VPN also saved me, as my IP was not leaked." [Participant 8]

Beyond direct actions by law enforcement, participants described how pro-regime political wings played an active role in intimidation—harassing protesters both physically

and verbally. The enforcement of censorship thus extended beyond official institutions to the social fabric itself, as peer networks and political affiliates became enforcers of silence. One participant recounted being beaten by members of a student wing after live-streaming the protest on Facebook. His testimony highlights how online visibility can immediately translate into physical vulnerability.

> "During the movement, I was on spot. I turned on a livestream on Facebook to show people the situation at our campus. After hours, my cousin, who is a member of the pro-regime wing, called me to delete the live stream or else I would be in trouble. Later that day, when I was going home, I was stopped by some pro-regime members, and they told me, 'He has been posting on Facebook about the protest,' and they beat me on the street and left me there. [...] Later, my cousin called me and told me, 'You have to stop posting, alright? See, you have a younger sister; if something bad happens to her, you are going to be liable because I warned you."' [Participant 4]

His experience illustrates how censorship blurred the boundary between political coercion and social obligation, where threats were delivered not only by strangers but also by kin. Familial ties became channels of intimidation, demonstrating how surveillance and discipline were woven into personal relationships and moral hierarchies. Threats over text and social media were also common among participants. Many received messages through Facebook Messenger or WhatsApp from anonymous accounts, often in multiple languages.

> "I got threats in my inbox—some even in Hindi, like stating 'I will take care of you.' A lot of them– threats in both Hindi and Bengali. I checked their profiles—no clue who they were, not in my friend list either. Maybe just because I was writing on Facebook during that time." [Participant 6]

Such messages reveal how digital harassment functioned as an extension of censorship, with coordinated groups intimidating targets and creating a sense of constant surveillance, where danger could emerge from any direction. The anonymity of these threats amplified their power, reinforcing a collective sense that online spaces were no longer safe for dissent.

Finally, several participants reported targeted network disruptions that went beyond the general internet blackout widely covered in the media. They noticed that specific protest hotspots—particularly university campuses—experienced localized disconnection, while neighboring areas remained online. These accounts suggest the use of network jammers or selective throttling as tools of control.

This pattern of targeted disconnection further illustrates the nature of censorship during the uprising: from physical violence and social pressure to infrastructural manipulation. The result was a layered ecosystem of control that constrained not only what people could say but also where, when, and how they could connect.

4.2 Digital Resilience to Mitigate Censorship

While the uprising was marked by widespread censorship and state-imposed blackouts, participants also revealed how ordinary citizens developed strategies of digital resilience to sustain communication and coordination. Amid surveillance and fear, they experimented with creative methods to protect themselves and their networks. Participants described how they repurposed everyday tools to circumvent control—using coded language, subtle hashtags, and layered privacy measures to share information. Some groups manually encrypted messages, while others relied on secure communication apps such as Signal or offline encryption software. Knowing that conventional platforms were monitored, they turned to cryptography and social ciphering—collective ways of concealing meaning—to maintain trust and operational safety.

One participant noted that Signal became a crucial medium for both coordination among protesters and emotional reassurance within activist networks, illustrating how encrypted communication tools served not just technical but also social resilience. Through these adaptive practices, citizens transformed surveillance infrastructures into sites of ingenuity, revealing that resilience under repression is not merely technological but profoundly relational.

> "Before the internet went down, we made a Signal group chat and also shared an AES-256 encryption key with our friends. We used this AES-256 encryption on our phones through an app. We encrypted our sensitive messages and sent them via traditional messaging during the internet blackout. This way, our messages were safe, and they were not exposed to any surveillance." [Participant 8]

> "In our department, all our colleagues were in a Signal group, where we would talk about our current situation and next plan. I was not aware of this app initially, then I came to know that this app was secure and encrypted, so we all used it to communicate." [Participant 3]

The same pattern of adaptation resonated among other participants, some of whom relied on privacy-oriented messaging apps for coordination. Many expressed a deep mistrust of mainstream messaging platforms such as Messenger or WhatsApp, fearing they were being monitored.

> " First, many of us had to use VPNs because the usual communication protocols were jammed. We couldn't make international calls. My sister was

> sick and in Bangkok with her husband—I couldn't reach them. Even for regular, non-political conversations, I didn't feel safe. So I shifted to Signal. I couldn't trust WhatsApp or Messenger anymore." [Participant 6]

Participants managing social media pages also described taking precautionary measures to ensure continuity despite the risk of arrest. They shared credentials with trusted allies or transferred administrative control to collaborators outside Bangladesh, allowing the movement's digital presence to persist even if local admins were detained. These practices illustrate how digital resilience extended beyond tools to strategies of *collective safeguarding*—where trust, delegation, and technical improvisation worked together to counter censorship and preserve the flow of information.

> "When we realized that we were being targeted, two of our group admins got arrested, and I thought of backup plans. First, I left the admin panel, which was my personal ID, then I made my page the admin of the group, as the page owner cannot be seen on Facebook. Also, I thought that if I get arrested, my page cannot be used to share information, so I made a friend of mine the admin of the page, who was in Japan [..] so the page can be operated from overseas" [Participant 11]

Beyond transferring admin roles, some participants also shared their account credentials and designated fallback operators to keep their pages active in case of arrest or disconnection. While they recognized that credential sharing posed a serious security risk, they viewed the uninterrupted flow of information as a higher priority. This trade-off reflects how, under conditions of repression, security and resistance often exist in tension—where collective continuity becomes more valuable than individual digital safety.

> "When people were getting arrested for posting on social media, I actually shared my Facebook credentials with a friend of mine. It was told that if I get arrested, he will take the lead and maintain the page." [Participant 14]

Participants also described a range of basic mitigation techniques to obscure their digital traces. They deleted sensitive messages and then filled chat histories with random text to make their inboxes appear ordinary. Others used burner email accounts, created "second spaces" on their phones to hide apps, or maintained multiple social media profiles for different purposes. These small, improvised acts reveal how digital resistance relied on mundane creativity, using everyday adjustments to balance caution, concealment, and the need to stay connected.

> "I used to use WhatsApp for our communication. But I used to unsend all the messages for both of us after a conversation. Then we would both delete all the 'Message is deleted' placeholder texts from both sides. After that, we used to send normal texts like 'How are you? How is the family, etc., so that my inbox does not look suspiciously empty." [Participant 10]

One participant highlighted how sharing information with international media required stronger anonymity. By using burner mail accounts and VPN, they avoided traceability while transmitting protest evidence.

> "During the protest, many of us believed that we should pass the information from Bangladesh to international media, and the only way to do that was to use e-mails. Now, if I use my institutional mail or personal mail, I can be tracked. So, I opened some burner emails on Gmail. I used to collect some data every day and send it to some international media newspapers. I also used VPN while sending them." [Participant 9]

Several participants described using the second space feature on their smartphones as a strategy to compartmentalize risk. In one space, they stored personal materials and evidence related to the protests; in the other, they maintained a "clean" profile containing only ordinary personal contents. They logged into social media through secondary accounts, filled galleries with benign photos, and even set up separate authentication methods to prevent accidental exposure. This dual-space tactic illustrates how participants transformed everyday smartphone features into tools of digital disguise, creating layered identities to navigate constant surveillance.

> "[..] I was interrogated during immigration. As mentioned before, my phone was confiscated, and they asked me to unlock it. I had dual space set up on my phone, and I know I cannot swap users in front of them, so I took a dual authentication method. If I use my right thumb, I will log into my actual space, and if I use my left thumb, I will log into my clean state." [Participant 16]

Some participants described additional safety measures to minimize the risk of being searched or having their devices confiscated. Before going outside, they backed up their data on laptops and wiped their phones completely to remove any trace of political activity. Others switched to basic feature phones when leaving home, reducing the likelihood of scrutiny or data extraction. These precautionary practices demonstrate how resilience often requires strategic downgrading—sacrificing digital convenience for the sake of personal security.

Several participants also described storing backups of sensitive data on physical devices such as SD cards or external hard drives, which they then hid to prevent seizure. This practice reflected a broader distrust of cloud-based storage, which many believed could be easily monitored or accessed by authorities. By turning to physical storage, participants asserted a form of offline security, reclaiming control over their data in a context where digital infrastructures had become sites of surveillance.

> "I switched to a button phone whenever I went outside. I don't trust any device connected to the internet. So I took a feature phone with me. No smartphone." [Participant 6]

> "After every day I went outside, in the protest, I would take pictures or record videos. But, I never kept them in my phone, or I could not trust the cloud platforms, if my phone is checked, they can be checked too. So, I stored all my data in an SD card and hid it in a torn fabric of my backpack." [Participant 17]

Participants also described how they circumvented censorship by manipulating hashtags and humor to disguise political content. Posts were crafted to appear pro-regime on the surface but carried critical or satirical undertones that spread opposition messages undetected. This strategic ambiguity allowed users to make banned hashtags trend while maintaining plausible deniability.

> "I really found this thing pretty amusing, how people manipulated the hashtags. There was a hashtag popular at that moment, '#Step_down', which was totally against the regime. But people would frame the hashtag in their post in a totally different way, like they would post 'Please do not use the hashtag #Step_down, this # Step_down is so inhumane, why would you use #Step_down', [..] This way, in a single post, people would use the hashtag like 10–20 times without getting noticed." [Participant 9]

These creative acts show how humor functioned not just as entertainment but as a security layer—'linguistic camouflage' that blended irony, satire, and political critique. By embedding truth in memes and playful language, protesters circulated information that felt harmless yet remained powerfully subversive.

Alongside these tactics, freelancers and digital workers developed pragmatic strategies to maintain connectivity and livelihood. Some chose to temporarily relocate abroad during the blackout to sustain communication with international clients and prevent financial losses.

> "If you look at that time, protesters used memes really effectively for digital activism. Even if they wrapped the truth in humor, the memes still spoke the truth. It helped them to spread information and truth." [Participant 6]

> "The blackout was for 10 days, so my friend told me that if I wanted to make my company survive, I had to leave Bangladesh and go to a neighboring country and work from there. It was true, I had already lost some clients because of being disconnected, and I could not take more risks. I felt bad though!" [Participant 16]

These accounts illustrate that digital resilience was not confined to political activism alone. For many, it extended to the economic sphere—where maintaining connectivity became a matter of survival, and migration itself emerged as a form of resistance against infrastructural repression.

4.3 Loss of Data Due to Surveillance and Fear

Participants frequently reported losing valuable data while attempting to protect themselves from surveillance. In their efforts to stay safe—backing up devices, deleting content, and wiping phones before leaving home—many accidentally erased important files, photos, and messages. The constant cycle of cleaning and concealment left little room for organized archiving, and fear often outweighed preservation. These losses reflect how censorship and surveillance not only restricted communication but also fragmented personal and collective memory, erasing traces of protest that might otherwise have served as evidence, history, or solidarity.

> "As I shared, I took a total backup of everything I had in my phone or PC to an SD Card and hid the SD card, and the time was messy. I had to move and change my location multiple times. In between all these, I forgot the exact place where I hid my SD Card last. I haven't found my SD Card yet, it had all the pictures and videos that I took during the protest." [Participant 17]

This experience was echoed by another participant who had systematically collected social media data as evidence of the protests. During the movement, he managed to back up some files from his phone to a flash drive, but after the protests ended, much of what he had gathered was missing. His account highlights how the fear of surveillance, rapid data deletion, and the constant need for concealment often led to unintended erasure, a loss not only of personal archives but of the collective record of resistance itself.

> "During the protest days, I used to collect photos and videos from Facebook and other social media

> [..]. I used to keep all backups on my pendrive. I had folders named as dates like '17th July'. After the protest was over, I found out that while taking backups, I lost many things; there were many dates missing. I will say, this happened because I was scared, I might have deleted it sometimes without backing up." [Participant 9]

One participant, who was arrested during the movement, used to keep secret folders on his phone. These secret folders contained all his data during the protest – how they planned to make the protest move forward, their research on the regime, and many other things. He lost his phone and could not find it yet, which led to severe data loss.

> "After the protest ended, we were bailed from prison. Now, my phone, which was taken away from me, had all the things I had done and collected during the protest. [..] It had a secret folder, which was locked, containing plans of the protest, texts, and notes.[..] I could not find the phone again! [..] So, I got nothing now." [Participant 13]

Another participant, the founder of the communication platform used during the blackout, also reported significant data loss after discovering that his IP address had been tracked and taken down by the service provider. Fearing further compromise, he not only deleted his files but also ensured that they could not be recovered through forensic tools. His actions reflect an extreme form of defensive deletion, where the instinct for self-protection trumps the desire to preserve digital evidence. This tension between safety and documentation illustrates how surveillance pressure compels individuals to erase traces of their own participation, producing both technological and historical loss.

> "When my IP was taken down, I was scared. And being scared, I formatted the hard disk that contained all the data of our platform [..]. I was so afraid that I just did not delete the hard disk, but also overwrote it multiple times using big game files that I had. I made sure that it cannot be recovered. Now, I understand that I lost many important statistics and data, which cannot be recovered anyhow." [Participant 15]

These accounts demonstrate that surveillance during the July 2024 Quota Reform Movement was not confined to state authorities, but was also diffused across laws, infrastructures, and social relations. Participants navigated a complex terrain where family members, peers, and pro-regime actors became enforcers of control, while censorship and fear reshaped the circulation of information. Yet alongside these pressures, protesters demonstrated resilience through technical improvisation, tactical communication, and everyday acts of resistance. These dynamics set the stage for our discussion, where we interpret these findings through the lens of surveillance theory and reconsider Bentham's Panopticon in light of a context where the watchers are everywhere.

5 Discussion

5.1 Rethinking Surveillance as Distributed Assemblage

Our analysis reveals that surveillance during the July 2024 uprising was not experienced uniformly across social ties. Instead, it emerged through various forms of relational obligation, in which family members, peers, and surroundings exerted pressure in different ways. Thus, local cultural emphasis on kinship and social ties further strengthened surveillance by extending it beyond state mechanisms into these intimate relations. However, the form, intensity, and costs of non-compliance varied depending on the nature of the relational tie. Family-based monitoring often involved coercive moral authority, whereas peer-based pressures took the form of political alignment, reputational threat, or fear of retaliation. Understanding these distinctions is central to conceptualizing how surveillance becomes woven into everyday life.

Existing frameworks help partially explain these dynamics. Bentham's Panopticon [19] and Foucault's notion of self-discipline [43] emphasize vertical, institutional power. Andrejevic's lateral surveillance [9], by contrast, captures peer-to-peer monitoring driven by curiosity, social comparison, or voluntary engagement. However, our participants described how local cultural norms and expectations underpinning various interpersonal relations exceeded these dynamics, such as coercive demands from parents who inspected phones, relatives who threatened consequences if live streams were not deleted, and kin networks that enforced silence out of fear of collective punishment. These were not instances of curiosity-driven watching but of relationally obligated compliance, where refusal risked punishment, shame, familial conflict, reputational harm, or physical violence.

To capture these interactions, we examine lateral surveillance through the lens of Global South movements, knowing that lateral surveillance assumes voluntary monitoring among peers situated on an equal plane, whereas our study foregrounds asymmetrical intimacy: relations where authority, dependence, emotional obligation, and shared vulnerability shape compliance. For example, family members can compel phone access in ways that peers cannot, or a parent can require the deletion of posts "for the family's protection." The use of the word 'can' in these examples does not imply that these practices are ethical or acceptable, but indicates that they are socio-culturally normalized. Relatedly, prior work examining surveillance in marginalized communities has shown how multiple intersecting identities—including religion, ethnicity, immigration status, and gender—create unique security and

privacy risks shaped by government surveillance, social tensions, and targeted harassment [1, 15]. While they touched on family and social observation of online dissent, we provide an in-depth examination of how surveillance within close social spheres is strengthened by sociocultural ties during political crises, revealing new threat models for security system design.

To signal this relational layering, we highlight how lateral surveillance within the movement operates through socially stratified horizontal relations. While surveillance occurs among non-state actors, it is shaped by sub-structural forces (e.g., kinship, obligation, dependency, gendered expectations, fear of collective punishment) that give certain actors coercive power over others. As a result, lateral surveillance in this context differs from generic peer monitoring, not through vertical authority, but through unequal relations embedded within ostensibly horizontal social ties. Rather than constituting a simple accumulation of watchers, this process reflects a socially stratified field in which intimacy itself becomes a vector of discipline.

In summary, our contribution clarifies how surveillance manifests differently across family, kin, and peer relations, and why these distinctions are important for understanding how protesters internalize discipline, navigate risks, and enact resilience in fragile contexts. This offers a sharper, relationally grounded perspective on everyday surveillance, extending existing work by foregrounding the obligatory nature of monitoring embedded in intimate ties.

5.2 Strategies to Support Local At-risk Protesters

Our findings generate a few deeper implications about activists' abilities to stay digitally safe. From our findings, it can be seen that many of our participants had a certain degree of technical knowledge, such as familiarity with encryption, knowledge of VPNs, and the Signal app, among others. This leads to an important research direction for future "surveillance" researchers regarding the adoption and improvisation of strategies for less tech-savvy activists. Prior research with BLM protesters reveals that the most common pieces of advice given to novice protesters are less understood and even more rarely followed [25]. This underscores the importance of design and technological interventions to keep these vulnerable people safe.

As reported by our participants, some of them were arrested or their houses got raided (P8, P10, P13, P18) during the movement. This reveals the susceptibilities associated with location tracking where Wi-Fi, Bluetooth, and GPS data from the smartphone could leak the location of a participant to law enforcement agencies. To mitigate this, a built-in "protester mode" can be integrated within the smartphone that would include features like automatically disabling Wi-Fi, Bluetooth, and location services, as well as automatically logging out of all apps, and clearing cached data. Furthermore, this mode could be configured to provide easy access to emergency contacts or a pre-loaded legal guide from the local civil liberties union.

However, the usable privacy and security community should focus on developing design solutions to support local activists, as smartphone manufacturers are often constrained by market demands, primarily responding to the needs of first-world users [36]. For example, as the US 5th Amendment protects a domestic detainee from being compelled to give their passcode [84], Android and iOS support the US users by providing a quick way to disable biometric authentication and force passcode authentication [56]. However, this design offers no protection for countries like Bangladesh, where authorities can force detainees to reveal their passcode. To help local protesters manually sanitize their phones, innovative design interventions are required.

As our data shows that device seizure is a common issue (P10, P16, P17) during protests in Bangladesh, prior work regarding "tiered" privacy in the context of domestic abuse in Bangladesh can be applied in this regard [5]. Using this model, a person can simultaneously create a "shared" account and a "secret" account, which contains data they are willing to share, and data they prefer to keep secret, respectively. One of our participants reported a similar strategy where they used their left thumb to log into their clean space and their right thumb to log into the actual profile. This design can be extended to support multiple passcodes, where each passcode is a prefix of the master passcode. For example, if the master passcode is "12345678", the first prefix "1234" would load the shared profile, the second prefix "123456" would load the intermediate profile that displays Facebook, Messenger, and Twitter, and only the master passcode would display all the apps, including VPNs and Signal.

Beyond these, the strand of work in usable privacy and security regarding defense against rubber hose attacks [23]– extraction of cryptographic or authentication secrets from a person by coercion or torture – can be applied to propose design interventions that support local protesters. Another important research direction could be exploring the adoption of linguistic camouflage (Section 4.2) among the protesters. Prior work on social steganography in Bangladesh demonstrates that communities apply different ciphering techniques to exchange information among peers in presence of outsiders [51], which could be leveraged as well to facilitate the exchange of sensitive and confidential information among the protesters.

5.3 The Ambivalence of Online Visibility

Our results can be directly linked to recent privacy studies conducted among marginalized communities in Bangladesh. Online visibility – an essential component to advance the goals of these communities – often enables their surveillance by law enforcement or other civilians. For the sex workers

in Bangladesh, online visibility is important to reach out to new clients; however, it also allows their "pseudo-husbands" to monitor their activities, embedding surveillance into care and dependence [101]. Similarly, while social media visibility of the Indigenous youth from the Chittagong Hill Tracts in Bangladesh helps them assimilate with the mainstream culture [98], it also subjects them to criticism from conservative elder family members. In response, these vulnerable people apply strategies such as maintaining dual profiles or adopting "linguistic camouflage" to manage their visibility to the intended audience [98, 101]. Navigating this ambivalence of online visibility has also been a major challenge for our participants, as they reported disguising dissent within pro-regime hashtags or posting content briefly before deleting it. These accounts illustrate how resilience is not only technical but also grounded in improvisation, secrecy, and humor. These practices resonate with Scott's *hidden transcripts* [53, 102] and de Certeau's *tactics* [30, 52], where marginalized groups disguise dissent and re-appropriate infrastructures.

As doxxing becomes increasingly common during social or political movements [57, 68], this issue of visibility has wider implications. When the protesters gain more visibility, they become susceptible to doxxing as it becomes easier to retrieve and publish their information with malicious intent. The defensive strategies adopted by these marginalized populations in the Global South, therefore, offer valuable insights for scholars globally. One common strategy adopted by the regimes to reduce the online visibility of the protesters is to order a nationwide internet blackout [48, 115]. Similar to our case, the regime in Myanmar enforced an internet blackout during the recent anti-military protests, which reveals the need for designing better offline applications during these turbulent times [48]. Our data provides in-depth accounts of how resistance is crafted through offline networks during internet blackouts and paves the way for future researchers to investigate this issue more deeply.

5.4 Lessons Learned

Researchers working in politically charged or censorship-heavy contexts may find our sampling process informative. We combined purposive sampling with snowball recruitment, which allowed us to reach highly involved participants while minimizing visibility and risk. In tightly bound contexts like the July Uprising, the depth of findings is more significant – a smaller, carefully targeted sample can offer a more accurate window into the experiences of a specific activist group. In contrast, collecting data from individuals who were not directly engaged in the movement would likely dilute, rather than strengthen, the analytical value of the dataset.

Furthermore, when a mass movement results in the overthrow of a regime – especially a long-standing one – the country undergoes a period of instability, in which an interim government usually steps in to restore law and order and make essential reforms to facilitate the next general election [7]. The initial few weeks are generally characterized by tension, unrest, and inundation of previously suppressed thoughts, and we recommend waiting for a period of time until a degree of stability is achieved before starting data collection. This also allows the participants to overcome trauma and develop a nuanced understanding of their own actions. In our case, the interviews began six months after the event and ended before its first anniversary – a timeline that seemed reasonable, given the observed psychological states of the participants and their ability to recall the incidents.

Finally, one co-author maintained a journal during the days of the movement to record its key technological aspects, which helped tremendously when preparing the questionnaire a few months later. We note that civic responsibility comes first, and it was prioritized over the record-keeping act by the co-author.

6 Limitations and Conclusion

This study, while offering deep insights into surveillance and resistance during Bangladesh's July 2024 Quota Reform Movement, has limitations. Our 23 interviews, though rich, cannot capture the full spectrum of experiences, especially of those tangentially involved or neutral. Participants shared accounts under political uncertainty, which may have shaped their disclosures. Finally, the focus on Bangladesh limits broad generalizability, though we have situated our findings within wider Global South contexts.

Despite these boundaries, our research makes theoretical and practical contributions. We highlight how lateral surveillance operates through kinship, peer, and everyday relations—not only vertical, state-driven repression. This foregrounds how infrastructures of fear and resilience are co-constructed in daily life, where trust and coercion blur. Our findings also demonstrate how resilience emerges through technical improvisation and cultural adaptation: encrypted tools, dual-phone strategies, panic-deletion mechanisms, satire, and coded speech. Resistance is sustained not merely through advanced technologies but through creativity, secrecy, and solidarity.

For design, these insights highlight urgent directions: systems supporting layered access control, rapid erasure, and offline or mesh-based communication capable of withstanding shutdowns. More broadly, our study underscores the need for infrastructures attuned to relational as well as institutional risks, especially where digital tools are both enablers of mobilization and instruments of repression.

In conclusion, surveillance in the Global South is distributed across infrastructures, laws, and intimate relations. Resilience is an ongoing negotiation blending technical ingenuity with cultural tactics—essential recognition for building technologies that safeguard civil liberties in repressive contexts.

Ethical Considerations

Our research protocol was reviewed and approved by the institutional review board of BRAC University.

Stakeholders and Their Exposure.

Study participants. The most directly affected stakeholders are the 23 study participants (including protesters, organizers, faculty members, and social media administrators) who discussed arrest, surveillance, device confiscation, and fear or coercion in a politically sensitive context. Publication creates residual risk that their practices could become more visible to hostile actors even with anonymization. Participants who built or administered protest-related infrastructure face greater exposure than those who participated more peripherally. We therefore report their accounts at a level of abstraction that preserves analytical value while avoiding operational specifics, as participant safety takes precedence over all other considerations.

Broader activist and civil society community. Publishing resilience practices can improve threat-model understanding for future activists and members of the civil society living under intense surveillance.

Security researchers and the S&P community. Researchers, platform designers, and the usable privacy and security community benefit from documentation of threat models involving coercion through intimate social relations and resilience under blackout conditions, both of which remain underexplored in security and privacy research.

Process-Related Risks and Mitigations.

All recordings were stored on local university machines without cloud backup, since cloud storage creates additional access points that could expose sensitive data to third parties. Data was manually transcribed and translated by native Bengali-speaking co-authors without automated tools, preserving contextual nuance while avoiding exposure to third-party services. Interviews were conducted months after the events, allowing participants more distance from immediate instability and trauma. In accordance with local customs in Bangladesh, in-person participants were offered light snacks and tea [51, 98]. We note that financial compensation is typically reserved for recruiting professional participants to discuss their occupational experiences [50, 101].

Why Conduct and Publish This Research?

The July 2024 uprising produced time-sensitive experiences of surveillance and digital resilience that are important for security and privacy research. Without careful documentation, these experiences risk being flattened into generic accounts of repression, obscuring how threats were also propagated through family, peers, and politically aligned social ties. We judged the research ethically justified because its value to the research community and to future protective design can be realized while keeping risk minimized through the safeguards described above.

Positionality Statement. Five co-authors witnessed the July 2024 Quota Reform Movement firsthand, either as students, faculty, or community members directly affected by the unfolding events. None of us is affiliated with any political party or organization, and we approached this study with a commitment to independence and neutrality in documenting participants' experiences. At the same time, we recognize that our values shape our research: as researchers and citizens, we believe strongly in civil liberties and stand against censorship, surveillance, and violence. This perspective informed both our sensitivity in engaging with participants and our responsibility to portray their narratives ethically, without exaggeration or political bias.

Open Science

Following usable privacy and security transparency practices [65], we have made our methodology, anonymized participant descriptions, consent form, and interview guidelines publicly available at https://doi.org/10.5281/zenodo.20438524. Due to IRB obligations and the sensitivity of interview data collected from activists and organizers in a politically volatile context, we are unable to release raw transcripts or identifiable materials.

A Relevant Legal Provisions in Bangladesh

This appendix provides excerpts (in English translation) of the legal provisions referenced in the main text. The translations are based on publicly available summaries and secondary sources [29, 38, 60].

A.1 Information and Communication Technology Act, 2006 (Section 57)

> Whoever intentionally publishes or transmits in electronic form any material which is fake, obscene, defamatory, or tends to deprave or corrupt its audience, or causes to deteriorate law and order, prejudice the image of the State or a person, or hurt religious beliefs, shall be punished with imprisonment, fine, or both.

A.2 Digital Security Act, 2018 (Relevant Sections)

Section 25. Transmission or publication of false, offensive, or threatening information via website or digital media that can tarnish the image of the nation, or cause enmity, hatred, or hostility.

Section 28. Publication or transmission of material that hurts religious values or sentiments.

Section 29. Publication or transmission of defamatory material.

Section 31. Publication or transmission of material that deteriorates law and order, prejudices communal harmony, or creates hostility, hatred, or antagonism between different classes or communities.

A.3 Cyber Security Act, 2023

The Cyber Security Act replaced the Digital Security Act in September 2023. Critics argue that it retains most of the repressive provisions of the DSA, with minor changes in penalties.

B Participant Demographic Table

Table 1: Participant Description

P#	Gender	Profession
1	Female	Faculty Member
2	Male	Faculty Member
3	Male	Sociologist, Faculty Member
4	Male	Student
5	Female	Student
6	Male	Faculty Member, Anthropologist
7	Female	Student
8	Male	Student
9	Male	Student
10	Female	Student
11	Male	Social Media Admin, Student
12	Male	Associate Professor
13	Male	Student
14	Male	Student, Social Media Manager, Journalist
15	Male	Student
16	Male	Student
17	Male	Student
18	Male	Student
19	Female	Lecturer
20	Female	Adjunct Lecturer
22	Female	Adjunct Lecturer
21	Female	Student
23	Female	Teacher

References

[1] Tanisha Afnan, Yixin Zou, Maryam Mustafa, Mustafa Naseem, and Florian Schaub. Aunties, strangers, and the {FBI}: Online privacy concerns and experiences of {Muslim-American} women. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 387–406, 2022.

[2] Sheetal D Agarwal, Michael L Barthel, Caterina Rost, Alan Borning, W Lance Bennett, and Courtney N Johnson. Grassroots organizing in the digital age: Considering values and technology in tea party and occupy wall street. *Information, Communication & Society*, 17(3):326–341, 2014.

[3] Md Shahin Ahmed. From legal protest to victory: A timeline of gen-z movement, 2025. URL: https://www.perspectivebd.com/article/from-legal-protest-to-victory:-a-timeline-of-gen-z-movement.

[4] Syed Ishtiaque Ahmed, Md Romael Haque, Jay Chen, and Nicola Dell. Digital privacy challenges with shared mobile phone use in bangladesh. *Proceedings of the ACM on Human-computer Interaction*, 1(CSCW):1–20, 2017.

[5] Syed Ishtiaque Ahmed, Md Romael Haque, Irtaza Haider, Jay Chen, and Nicola Dell. " everyone has some personal stuff" designing to support digital privacy with shared mobile phone use in bangladesh. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2019.

[6] Martin R Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Mareková. Collective information security in {large-scale} urban protests: The case of hong kong. In *30th USENIX security symposium (USENIX Security 21)*, pages 3363–3380, 2021.

[7] Amira Aleya-Sghaier. The tunisian revolution: The revolution of dignity. *The Journal of the Middle East and Africa*, 3(1):18–45, 2012.

[8] Monica Anderson, Michael Barthel, Andrew Perrin, and Emily A. Vogels. #blacklivesmatter surges on twitter after george floyd's death, Jun 2020. URL: https://www.pewresearch.org/short-reads/2020/06/10/blacklivesmatter-surges-on-twitter-after-george-floyds-death/.

[9] Mark Andrejevic. The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, 2(4), 2004.

[10] Mark Andrejevic. The discipline of watching: Detection, risk, and lateral surveillance. *Critical Studies in Media Communication*, 23(5):391–407, 2006.

[11] Mark Andrejevic. Surveillance in the big data era. In *Emerging Pervasive Information and Communication Technologies (PICT) Ethical Challenges, Opportunities and Safeguards*, pages 55–69. Springer, 2013.

[12] Mark Andrejevic. Automating surveillance. *Surveillance & society*, 17(1/2):7–13, 2019.

[13] Mark Andrejevic, Hugh Davies, Ruth DeSouza, Larissa Hjorth, and Ingrid Richardson. Situating 'careful surveillance'. *International Journal of Cultural Studies*, 24(4):567–583, 2021.

[14] Tamim Anowar. The role of social media in activism in bangladesh: Transforming organization, awareness, and mobilization. *Awareness, and Mobilization (February 06, 2024)*, 2024.

[15] Arjun Arunasalam, Habiba Farrukh, Eliz Tekcan, and Z Berkay Celik. Understanding the security and privacy implications of online toxic content on refugees. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 4373–4390, 2024.

[16] Aanandita Bali and Shuo Niu. Voices in videos: How youtube is used in# blm and# stopaapihate movements. *Platforms*, 3(2):8, 2025.

[17] Elmond Bandauko. 'shadowing the state': Subaltern surveillance and the rhythms of everyday resistance. *Dialogues in Human Geography*, page 20438206251398537, 2025.

[18] James R Barker and George Cheney. The concept and the practices of discipline in contemporary organizational life. *Communications Monographs*, 61(1):19–43, 1994.

[19] Jeremy Bentham. *The panopticon writings*. Verso Books, 2020.

[20] Patrick Bergemann. Denunciation and social control. *American Sociological Review*, 82(2):384–406, 2017.

[21] Marty Berger and David A Sklansky. Crime, community, and the shadow of the virtual. *U. Ill. L. Rev.*, page 1607, 2023.

[22] Julia Bleckner. *After the Monsoon Revolution*. January 2025. URL: https://www.hrw.org/report/2025/01/27/after-monsoon-revolution/roadmap-lasting-security-sector-reform-bangladesh.

[23] Hristo Bojinov, Daniel Sanchez, Paul Reber, Dan Boneh, and Patrick Lincoln. Neuroscience meets cryptography: crypto primitives secure against rubber hose attacks. *Commun. ACM*, 57(5):110–118, May 2014. doi:10.1145/2594445.

[24] R Boyatzis. *Transforming qualitative information: Thematic analysis and code development*. Sage, 1998.

[25] Maia J Boyd, Jamar L Sullivan Jr, Marshini Chetty, and Blase Ur. Understanding the security and privacy advice given to black lives matter protesters. In *Proceedings of the 2021 CHI conference on human factors in computing systems*, pages 1–18, 2021.

[26] Michael Buerger. The politics of third-party policing. *Crime prevention studies*, 9:89–116, 1998.

[27] Bart Cammaerts. Social media and activism. *Journalism*, pages 1027–1034, 2015.

[28] Steve Campbell, Melanie Greenwood, Sarah Prior, Toniele Shearer, Kerrie Walkem, Sarah Young, Danielle Bywaters, and Kim Walker. Purposive sampling: complex or simple? research case examples. *Journal of research in Nursing*, 25(8):652–661, 2020.

[29] Center for Justice and Accountability. Bangladesh's zombie cyber security law: A comparative analysis of ict act, dsa, and csa, 2024. URL: https://cfj.org/wp-content/uploads/2024/11/Bangladesh-ICT-Act-Report_November-2024-1.pdf.

[30] Michel de Certeau and Steven Rendall. The practice of everyday life. *(No Title)*, 1984.

[31] Janakee Chavda and Janakee Chavda. More than twice as many americans support than oppose the #metoo movement, April 2025. URL: https://www.pewresearch.org/social-trends/2022/09/29/more-than-twice-as-many-americans-support-than-oppose-the-metoo-movement/.

[32] Josh Chin and Liza Lin. *Surveillance state: inside China's quest to launch a new era of social control*. St. Martin's Press, 2022.

[33] James J Chriss. *Social control: An introduction*. John Wiley & Sons, 2022.

[34] Juliet Corbin and Anselm Strauss. *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications, 2014.

[35] Jonathan M Cox. The source of a movement: Making the case for social media as an informational source using black lives matter. *Ethnic and Racial Studies*, 40(11):1847–1854, 2017.

[36] Alaa Daffalla, Lucy Simko, Tadayoshi Kohno, and Alexandru G Bardas. Defensive technology use by political activists during the sudanese revolution. In *2021 IEEE symposium on security and privacy (SP)*, pages 372–390. IEEE, 2021.

[37] Gilles Deleuze. Postscript on the societies of control. In *Surveillance, crime and social control*, pages 35–39. Routledge, 2017.

[38] Dhaka Tribune. How section 57 morphed into digital security act provisions. *Dhaka Tribune*, 2018. URL: https://www.dhakatribune.com/bangladesh/laws-rights/152724/how-section-57-morphed-into-digital-security-act.

[39] Henrike Donner and Victoria Goddard. Kinship and the politics of responsibility: An introduction. *Critique of Anthropology*, 43(4):331–364, 2023.

[40] John DH Downing. Looking back, looking ahead: What has changed in social movement media since the internet and social media? In *The Routledge companion to media and activism*, pages 19–27. Routledge, 2018.

[41] Jennifer Earl, Thomas V. Maher, and Jennifer Pan. The digital repression of social movements, protest, and activism: A synthetic review. *Science Advances*, 8(10):eabl8198, 2022. URL: https://www.science.org/doi/abs/10.1126/sciadv.abl8198, arXiv:https://www.science.org/doi/pdf/10.1126/sciadv.abl8198, doi:10.1126/sciadv.abl8198.

[42] Ilker Etikan, Sulaiman Abubakar Musa, Rukayya Sunusi Alkassim, et al. Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics*, 5(1):1–4, 2016.

[43] Michel Foucault. *Discipline and punish: The birth of the prison*. Vintage, 2012.

[44] Maša Galič, Tjerk Timan, and Bert-Jaap Koops. Bentham, deleuze and beyond: An overview of surveillance theories from the panopticon to participation. *Philosophy & Technology*, 30(1):9–37, 2017.

[45] Philip Garrahan and Paul Stewart. The nissan enigma: Flexibility at work in a local economy. 1994.

[46] Barney Glaser and Anselm Strauss. *Discovery of grounded theory: Strategies for qualitative research*. Routledge, 2017.

[47] William J Goode. *The celebration of heroes: Prestige as a social control system*. Univ of California Press, 2022.

[48] Laura Gianna Guntrum. Keyboard fighters: The use of icts by activists in times of military coup in myanmar. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, pages 1–19, 2024.

[49] Kevin D Haggerty and Richard V Ericson. The surveillant assemblage. *Surveillance, crime and social control*, pages 61–78, 2017.

[50] SM Taiabul Haque, Rayhan Rashed, Mehrab Bin Morshed, Md Main Uddin Rony, Naeemul Hassan, and Syed Ishtiaque Ahmed. Exploring the tensions between the owners and the drivers of uber cars in urban bangladesh. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1):1–25, 2021.

[51] SM Taiabul Haque, Pratyasha Saha, Muhammad Sajidur Rahman, and Syed Ishtiaque Ahmed. Of ulti,'hajano', and" matachetar otanetak datam" exploring local practices of exchanging confidential and sensitive information in urban bangladesh. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–22, 2019.

[52] Matt Hills. Strategies, tactics and the question of un lieu propre: What/where is "media theory"? *Social Semiotics*, 14(2):133–149, 2004.

[53] Emily Horowitz. Resistance reimagined: Disability and the hidden transcripts of everyday resistance. Master's thesis, University of Illinois at Chicago, 2020.

[54] Reham Hosny. Shifting paradigms of cultural expression: Toward a critical framework for arab digital cultural studies. *Faculty of Arts Journal–Suez University*, 2025.

[55] Reham Hosny and Mohamed A Nasef. Lexical algorithmic resistance: Tactics of deceiving arabic content moderation algorithms on facebook. *Big Data & Society*, 12(2):20539517251318277, 2025.

[56] Kendall Howell. The fifth amendment, decryption and biometric passcodes, January 2023. URL: https://www.lawfaremedia.org/article/fifth-amendment-decryption-and-biometric-passcodes.

[57] Laura Huey, Lorna Ferguson, and Zachary Towns. "cops need doxxed": Releasing personal information of police officers as a tool of political harassment. *Crime & Delinquency*, 71(3):714–739, 2025.

[58] Azra Humayra. Experiencing july 15 as a student. *The Daily Star*, July 2024. URL: https://www.thedailystar.net/campus/campus/news/experiencing-july-15-student-3658416.

[59] Alice Ievins. 'perfectly individualized and constantly visible'? lateral tightness in a prison holding men convicted of sex offences. *Incarceration*, 1(1):2632666320936433, 2020.

[60] Amnesty International. Bangladesh: Interim government must restore freedom of expression in bangladesh and repeal cyber security act, August 2024. URL: https://www.amnesty.org/en/latest/news/2024/08/bangladesh-interim-government-must-restore-freedom-of-expression-in-bangladesh-and-repeal-cyber-security-act/.

[61] Jonathan Jackson, Krisztián Pósch, Thiago R Oliveira, Ben Bradford, Sílvia M Mendes, Ariadne Lima Natal, and André Zanetic. Fear and legitimacy in são paulo, brazil: Police–citizen relations in a high violence, high fear city. *Law & society review*, 56(1):122–145, 2022.

[62] Al Jazeera. Bangladeshi rap, memes helped oust hasina — now they're reshaping politics. *Al Jazeera*, July 2025. URL: https://www.aljazeera.com/features/2025/7/11/rap-memes-graffiti-bangladeshs-new-political-tools-a-year-after-hasina.

[63] Quentin Key. Sanctuary of the voiceless: Examining tik-tok as a political landscape. Master's thesis, University of Arkansas, 2025.

[64] Oleg Kharkhordin. The collective and the individual in russia: a study of practices, 1999.

[65] Jan H Klemmer, Juliane Schmüser, Fabian Fischer, Jacques Suray, Jan-Ulrich Holtgrave, Simon Lenau, Byron M Lowens, Florian Schaub, and Sascha Fahl. How transparent is usable privacy and security research? a {Meta-Study} on current research transparency practices. In *34th USENIX Security Symposium (USENIX Security 25)*, pages 5967–5986, 2025.

[66] Yong Ming Kow, Bonnie Nardi, and Wai Kuen Cheng. 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*, pages 1–12, 2020.

[67] Rahim Kurwa. Building the digitally gated community: The case of nextdoor. *Surveillance & Society*, 17(1/2):111–117, 2019.

[68] Carmen Lee. Doxxing as discursive action in a social movement. *Critical Discourse Studies*, 19(3):326–344, 2022.

[69] Francis LF Lee, Hsuan-Ting Chen, and Michael Chan. Social media use and university students' participation in a large-scale protest campaign: The case of hong kong's umbrella movement. *Telematics and informatics*, 34(2):457–469, 2017.

[70] Primo Levi. *The drowned and the saved*. Simon and Schuster, 2017.

[71] Alison Lewis. A state of secrecy: stasi informers and the culture of surveillance. 2021.

[72] Rui Li, Zhijun Chen, Huihua Zhang, and Jinlian Luo. How do authoritarian leadership and abusive supervision jointly thwart follower proactivity? a social control perspective. *Journal of Management*, 47(4):930–956, 2021.

[73] Merlyna Lim. Clicks, cabs, and coffee houses: Social media and oppositional movements in egypt, 2004–2011. *Journal of communication*, 62(2):231–248, 2012.

[74] Sylvia Lu. Data privacy, human rights, and algorithmic opacity. *Cal. L. Rev.*, 110:2087, 2022.

[75] Anna Ricarda Luther, Hendrik Heuer, Stephanie Geise, Sebastian Haunss, and Andreas Breiter. Social media for activists: Reimagining safety, content presentation, and workflows. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, pages 1–18, 2025.

[76] David Lyon. Surveillance. *Internet Policy Review*, 11(4):1–18, 2022.

[77] Mahmood Mamdani. Historicizing power and responses to power: Indirect rule and its reform. *Social research*, pages 859–886, 1999.

[78] Håvard Rustad Markussen. Conceptualising the smartphone as a security device: Appropriations of embodied connectivity at the black lives matter protests. *Critical Studies on Security*, 10(2):70–84, 2022.

[79] Iyanna C Marshall, Lillian A Hammer, Cassi R Springfield, and Kelsey A Bonfils. Activism in the digital age: the link between social media engagement with black lives matter-relevant content and mental health. *Psychological reports*, 127(5):2220–2244, 2024.

[80] Alex Martins. Reimagining equity: redressing power imbalances between the global north and the global south. *Gender & Development*, 28(1):135–153, 2020.

[81] Lorraine Mazerolle, Kevin Petersen, Michelle Sydes, and Janet Ransley. *Partnerships in Policing: How Third Parties Help Police to Reduce Crime and Disorder*. Cambridge University Press, 2025.

[82] Colin McFarlane. Translocal assemblages: Space, power and social movements. *Geoforum*, 40(4):561–567, 2009.

[83] Lucas Melgaço. Recursive surveillance and the persistence of authoritarian surveillance in brazil. *Surveillance & Society*, 23(1):140–144, 2025.

[84] Justin Meyers. How to quickly disable fingerprints & smart lock in android pie for extra security, March 2018. URL: https://android.gadgethacks.com/how-to/quickly-disable-fingerprints-smart-lock-android-%20pie-for-extra-security-0183475/.

[85] Jean Christopher Mittelstaedt. The grid management system in contemporary china: Grass-roots governance in social surveillance and service provision. *China Information*, 36(1):3–22, 2022.

[86] Jimin Mun, Cathy Buerger, Jenny T Liang, Joshua Garland, and Maarten Sap. Counterspeakers' perspectives: Unveiling barriers and ai needs in the fight against online hate. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, pages 1–22, 2024.

[87] Allen Munoriyarwa. The militarization of digital surveillance in post-coup zimbabwe:'just don't tell them what we do'. *Security Dialogue*, 53(5):456–474, 2022.

[88] Sara Naderi. The banality of a medium: Iran's "woman, life, freedom" movement in the social media mirror. *Atlantis*, 46(1):9–23, 2025.

[89] Constance A Nathanson. Peer surveillance and patient orientation in a pediatric out-patient clinic. *Human Organization*, 30(3):255–265, 1971.

[90] Netra News. Bangladesh reinstates fixed-line internet at select locations, July 2024. URL: https://netra.news/2024/bangladesh-reinstates-fixed-line-internet-select-locations/.

[91] Office of the United Nations High Commissioner for Human Rights (OHCHR). Justice and accountability: "woman, life, freedom" protests. https://www.ohchr.org/en/stories/2025/04/justice-and-accountability-woman-life-freedom-protests, April 2025. Accessed: 2025-08-29.

[92] Suay M Özkula and Paul J Reilly. Where is the global south? northern visibilities in digital activism research. *Social Media+ Society*, 10(4):20563051241299835, 2024.

[93] Andrea Purdeková. "mundane sights" of power: the history of social monitoring and its subversion in rwanda. *African Studies Review*, 59(2):59–86, 2016.

[94] Md. Zahidur Rabbi. The daily star, Aug 2025. URL: https://www.thedailystar.net/tech-startup/news/how-gen-z-kept-connected-after-the-internet-shutdown-3956001.

[95] Tohidul Islam Raso, Suhadha Afrin, Miraj Ahmed Chowdhury, Maria Xynou, and Elizaveta Yachmeneva. The longest silence: Internet shutdowns during bangladesh's 2024 uprising, jul 2025. Accessed: 2025-09-12. URL: https://ooni.org/post/2025-bangladesh-report/.

[96] RMTGP Rathnayaka. Role of social media and online news in 2022 sri lankan riots and utilization of ooda loop based osint framework. 2023.

[97] Yasamin Rezai. Performing iran online: Digital poetics and feminist activism in the woman life freedom movement. *Journal of Gender Studies*, pages 1–18, 2024.

[98] Ishmam Bin Rofi, Mashiyat Mahjabin Eshita, Avijoy Chakma, Md Sabbir Ahmed, SM Taiabul Haque, and Jannatun Noor. The good, the bad and the ugly: The opportunities, challenges and the mitigation strategies of the young indigenous social media users of the chittagong hill tracts in bangladesh. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, pages 1–22, 2025.

[99] Leah Namisa Rosenbloom. Activists want better, safer technology. *arXiv preprint arXiv:2209.01273*, 2022.

[100] Julia Ryng, Guillemette Guicherd, Judy Al Saman, Priyanka Choudhury, and Angharad Kellett. Internet shutdowns: a human rights issue. *The RUSI Journal*, 167(4-5):50–63, 2022.

[101] Pratyasha Saha, Nadira Nowsher, Ayien Utshob Baidya, Nusrat Jahan Mim, Syed Ishtiaque Ahmed, and SM Taiabul Haque. Computing and the stigmatized: Trust, surveillance, and spatial politics with the sex workers in bangladesh. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, pages 1–22, 2024.

[102] James C Scott. *Domination and the arts of resistance: Hidden transcripts*. Yale university press, 1990.

[103] James C Scott. *Seeing like a state: How certain schemes to improve the human condition have failed*. yale university Press, 2020.

[104] Janet Semple. *Bentham's Prison: A Study of the Panopticon Penitentiary: A Study of the Panopticon Penitentiary*. Clarendon Press, 1993.

[105] Graham Sewell. Organization, employees and surveillance. In *Routledge handbook of surveillance studies*, pages 303–312. Routledge, 2012.

[106] Ali Asif Shawon. Survey: Most youths prefer social media for news updates. *Dhaka Tribune*, January 2025. URL: https://www.dhakatribune.com/bangladesh/372105/survey-most-youths-prefer-social-media-for-news.

[107] Abu Bakar Siddik. Bangladesh's july revolution: Analyzing the 2024 movement for free speech and democracy. *Available at SSRN 5043479*, 2024.

[108] Parama Sigurdsen and Ravi Iyer. A double-edged sword: The role of social media in the 2024 political uprising in bangladesh, September 2024. URL: https:

//www.techpolicy.press/a-double-edged-sword-the-role-of-social-media-in-the-2024-political-uprising-in-bangladesh/.

[109] Joseph Jay Sosa. Epistemic doubt and affective certainty: counting homotransphobia in brazil. *Theory and Society*, 52(1):95–117, 2023.

[110] Al Jazeera Staff. What's behind bangladesh's violent quota protests? *Al Jazeera*, July 2024. URL: https://www.aljazeera.com/news/2024/7/16/whats-behind-bangladeshs-violent-quota-protests.

[111] Ann Laura Stoler. *Race and the education of desire: Foucault's history of sexuality and the colonial order of things*. Duke University Press, 1995.

[112] Ann Laura Stoler. Colonial archives and the arts of governance. *Archival science*, 2(1):87–109, 2002.

[113] Muktita Suhartono and Sui-Lee Wee. Indonesia's leader says he will bow to some protester demands after riots. *The New York Times*, Aug 2025. URL: https://www.nytimes.com/2025/08/31/world/asia/indonesia-protest-politicians-ransack-loot.html.

[114] Achhiya Sultana, Dipto Das, Saadia Binte Alam, Mohammad Shidujaman, and Syed Ishtiaque Ahmed. A civics-oriented approach to understanding intersectionally marginalized users' experience with hate speech online. In *Proceedings of the 13th International Conference on Information & Communication Technologies and Development*, pages 57–68, 2024.

[115] Zinnat Sultana, Miss Rokeya Akter, Tanveer Ehsanur Rahman, Hasan Shahid Ferdous, Teresa Wulandari, M Ashraful Amin, Syed Ishtiaque Ahmed, and Sharifa Sultana. Internet disconnection as a risk to cross-border human rights. In *Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, pages 1–7, 2025.

[116] Maria Dolores C Tongco. Purposive sampling as a tool for informant selection. 2007.

[117] Harry C Triandis. Individualism-collectivism and personality. *Journal of personality*, 69(6):907–924, 2001.

[118] Justin Turner and Travis Milburn. Citizen empowerment as a police force multiplier: Reproducing social domination through a 21st century personal safety app. *Crime, Media, Culture*, 21(1):27–45, 2025.

[119] Safaa Turner-Rahman and University of Washington. *Networks of Control: National and Transnational Digital Repression in Bangladesh*. July 2025. URL: https://jsis.washington.edu/news/national-and-transnational-digital-repression-in-bangladesh/.

[120] Al Jazeera Investigative Unit and Will Thorne. 'shoot them': Sheikh hasina ordered firing on bangladesh protesters in 2024. *Al Jazeera*, July 2025. URL: https://www.aljazeera.com/news/2025/7/24/shoot-them-sheikh-hasina-ordered-firing-on-bangladesh-protesters-in-2024.

[121] Lior Volinz. Authoritarian surveillance: An introduction. *Surveillance & Society*, 23(1):112–116, 2025.

[122] Katie Washington and Rachel Marcus. Hashtags, memes and selfies: can social media and online activism shift gender norms. *ALIGN Report. London: Overseas Development Institute*, 2022.

[123] David Murakami Wood. Beyond the panopticon? foucault and surveillance studies. In *Space, knowledge and power*, pages 245–263. Routledge, 2016.

[124] William Lafi Youmans and Jillian C York. Social media and the activist toolkit: User agreements, corporate interests, and the information infrastructure of modern social movements. *Journal of communication*, 62(2):315–329, 2012.

[125] Shoshana Zuboff. The secrets of surveillance capitalism. *Frankfurter Allgemeine Zeitung*, 5:2016, 2016.