"They Don't Leave Us Alone Anywhere We Go": Gender and Digital Abuse in South Asia

Nithya Sambasivan
Google
USA
nithyasamba@google.com

Amna Batool
Information Technology University
Pakistan
batool.amna@itu.edu.pk

Nova Ahmed
North South University
Bangladesh
nova.ahmed@northsouth.edu

Tara Matthews
Independent Researcher
USA
taramatthews@gmail.com

Kurt Thomas
Google
USA
kurtthomas@google.com

Laura Sanely Gaytán-Lugo
Universidad de Colima
Mexico
laura@ucol.mx

David Nemer
University of Kentucky
USA
david.nemer@uky.edu

Elie Bursztein,
Elizabeth Churchill,
Sunny Consolvo
Google
USA
{elieb,echurchill,sconsolvo}@google.com

ABSTRACT

South Asia faces one of the largest gender gaps online globally, and online safety is one of the main barriers to gender-equitable Internet access [GSMA, 2015]. To better understand the gendered risks and coping practices online in South Asia, we present a qualitative study of the online abuse experiences and coping practices of 199 people who identified as women and 6 NGO staff from India, Pakistan, and Bangladesh, using a feminist analysis. We found that a majority of our participants regularly contended with online abuse, experiencing three major abuse types: *cyberstalking*, *impersonation*, and *personal content leakages*. Consequences of abuse included emotional harm, reputation damage, and physical and sexual violence. Participants coped through informal channels rather than through technological protections or law enforcement. Altogether, our findings point to opportunities for designs, policies, and algorithms to improve women's safety online in South Asia.

CCS CONCEPTS

• **Human-centered computing → Empirical studies in HCI**.

KEYWORDS

Online abuse; Privacy; Stalking; Impersonation; Leakages; India; Pakistan; Bangladesh; Women; Coping; Impacts

ACM Reference Format:
Nithya Sambasivan, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Sanely Gaytán-Lugo, David Nemer, and Elie Bursztein,, Elizabeth Churchill,, Sunny Consolvo. 2019. "They Don't Leave Us Alone Anywhere We Go": Gender and Digital Abuse in South Asia. In *CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019, Glasgow, Scotland Uk.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3290605.3300232

CHI 2019, May 4–9, 2019, Glasgow, Scotland Uk

ACM ISBN 978-1-4503-5970-2/19/05.
https://doi.org/10.1145/3290605.3300232

1 INTRODUCTION

The Internet is expanding its reach across South Asia, but only 29% of users from India are women [47]. Likewise, women in South Asia are 26% less likely than South Asian men to own a phone and 70% less likely to connect to the Internet via a mobile device [41]. One of the largest barriers to gender-equitable participation in this region is online safety (among other barriers like affordability and relevance), driven in part by fear of contending with harassment [41] and risks to one's reputation [54]. Consequences of online abuse can be extreme. For example, Qandeel Baloch, a social media celebrity in Pakistan, was murdered by her brother in 2016 for posting selfies that he perceived to mar their family's honor [39]. In another incident, Vinupriya in India committed suicide after her social media profile photo was stitched to a semi-nude body and spread virally [67]. Naina Rahman of Bangladesh attempted suicide after a similar impersonation incident in 2017 [57]. The fear surrounding these

events further reduces the online participation of women in an already gender-unequal Internet context [41].

The specter of online abuse is not unique to South Asian women. People across the Internet contend with a gamut of threats including harassment [6], bullying [31], revenge porn [26], and doxxing [21]. Compared to men, women are more likely to be targets for online abuse [25, 55, 96]. Despite this breadth of prior work, existing studies largely focus on Internet users in the United States and Western Europe (*e.g.*, [14, 19, 21, 22, 26, 29, 96]). However, abuse experiences do not generalize uniformly across the world. South Asia represents a distinct context where gender inequality is high [34], technology is newly emerging [61], and cultural norms and expectations are unique to the region [83].

In this paper, we aim to show the manner in which abuse is articulated online in the everyday, gendered lives of women in India, Pakistan, and Bangladesh. We draw from qualitative interviews with 199 cisgender and non-cisgender members who identified as women and 6 staff members at four NGOs that provide services to abuse victims in the region. 'Online abuse' refers to privacy invasions, malicious activity, harm tactics, and other forms of marginalization that participants reported experiencing. We recruited participants across social classes, religions, and ages to capture a cross-section of experiences and perspectives. We did not intentionally sample victims of abuse, but instead sought out general technology users. Our study addresses three research questions: (1) what types of online abuse do South Asian women face and how pervasively?; (2) how is the online abuse coped with?; and (3) what are the impacts of online abuse? These questions provide a unique lens into the experience, prevalence, and severity of abuse facing an otherwise newly emerging population of Internet users. We employ a South Asian feminist lens to engage with the research and its implications.

We found that a majority (72%) of our participants reported experiencing online abuse, especially on social media platforms. We collated these experiences into three consistent abuse types. *Cyberstalking* involved an abuser initiating unwanted contact (reported by 66% of participants). *Impersonation* involved an abuser creating a malicious likeness of the victim without their consent (15%). *Personal Content Leakages* involved an abuser non-consensually exposing the participant's online activity in unwanted social contexts (14%). We found that younger and rural, sexual minorities, and low-income participants reported abuse more commonly. Cyberstalking was more commonly reported by Indian participants, and impersonation and personal content leakages were higher among Pakistani and Bangladeshi participants.

Abuse in South Asia is materially different from what is reported in other geographic or cultural contexts. Even seemingly minor infractions, such as a stranger lifting a participant's profile photo or leaking their name, carried significant consequences. Participants cited emotional harm, reputation harm, romantic coercion, and domestic violence as consequences of online abuse. Taken as a whole, prevalence and severity of the abuse types we identify are substantively different from other contexts due to the influence of local norms and power relations.

Participants largely did not turn to law enforcement or in-app reporting on social media platforms for support in online abuse situations. Instead, they relied on informal solutions; for example, half the participants reached out to friends or family for support. Other coping techniques included limiting the information provided on social profiles, posting non-face photos on their profiles, and using mechanisms to establish trust with contacts online.

In summary, we make two primary contributions. We present a qualitative study examining the online abuse experiences of South Asian women, the consequences they face due to abuse, and their coping practices. Secondly, we discuss the implications of our results in enabling technology creators to design their systems and policies to better account for these threats in South Asia.

2 RELATED WORK

Types of online abuse attacks

Prior research has explored abuse online in the context of sexual harassment [78], cyberstalking [11], catfishing [52], revenge porn [26], doxxing [21], sextortion [99, 100], intimate partner violence [30, 31, 36, 37, 60, 89, 101], and more. Participants from research on abuse included school children [32], college students [33], online gamers [44, 49, 94], celebrities [80], Wikipedia contributors [27], dating site users [59], and intimate partner abuse survivors [30, 31, 36, 37, 60, 89, 101]. Women experience a wider variety of online abuse than men, and are more likely to be angry, worried, or scared as a result [55]; with younger women [78, 96], and sexual and racial minorities [31, 78] being more susceptible to online abuse. Across the abuse literature, there has been an emphasis largely on North American and Western European populations. We now highlight related work on cyberstalking, impersonation, and personal data leakages—the three main abuse types articulated by our participants.

Cyberstalking. Stalking encompasses a range of behaviors initiated by an individual who engages in a pattern of harassing or threatening behavior [15], manifesting as following a person, making harassing phone calls, leaving written messages, or vandalizing property [93]. Cyberstalking is where the Internet is used to identify and target victims [11]. A 2017 PEW survey conducted with 4,248 U.S. adults notes that 7% reported experiencing cyberstalking [78].

Impersonation. Impersonation is described as "pretending to be someone else and sending or posting material to get that person in trouble or danger or to damage that person's

reputation or friendships" [98]. Impersonation can be harmful to both the people who interact with the profile and to the person whose identity is co-opted [52]. Impersonation occurs in the form of stolen identities of real people [91], celebrities [80], and bots [40]. Attacks can manifest as false social identities [91], deepfakes [80], phone call spoofing [10], or e-mail spoofing [38]. Impersonation can result in financial loss [86, 91], romantic loss [86], and emotional withdrawal [86]. Lenhart et al. in their 2016 survey with 3,002 Americans report that 6% experienced impersonation [55].

Personal content leakages. Doxxing is the outing of private information, such as intimate photos or finances, nonconsensually to the public [13]. Doxxing is instigated by factors like public vigilantism [3, 21], offline harassment [81], and shaming [13]. Revenge porn is the distribution of private, sexually-explicit images of individuals without their consent [5], making the victim a 'sex object' with a damaged reputation [43]. In Lenhart et al.'s 2016 survey, revenge porn was reported by 2% of respondents [55].

Strategies for coping with abuse

Research on coping practices has also focused mainly on Western populations. Unabated, victims tend to ignore low-severity abuse [78], while more severe forms can result in victims withdrawing from platforms [25, 27, 29, 35, 65, 96]; self-censoring, [70]; feeling anxiety [73]; and committing suicide [90]. To cope with abuse, victims may adopt anonymous and gender-neutral identities, self-limit content, use humor, and avoid communication with others [35, 54, 96, 97]. Some rely on reactive strategies like ignoring abuse, confronting abusers, avoiding location sharing, editing privacy settings, and deleting accounts [49, 55, 97, 100]. Social support may be sought through through online communities [14, 29, 35] and women-only spaces [12]. A sizeable 27% of victims reported abuse to technology platforms in Lenhart et al.'s 2016 survey [55]. However platforms may lack consistency in policies and there may be non-transparency in responses to reports of abuse [19, 74]. Prior research in the West shows that abuse victims rely heavily on technological options like self-limiting content, reporting abuse, or modifying privacy settings [35, 55, 96]. For more severe incidents, victims seek support from law enforcement [100]. Abuse laws are seen as less supportive of women, but restraining orders are sometimes used [25, 58, 58]. Victims may also rely on women's shelters for severe abuse [30, 55, 60].

Similarities across these prior results from the West and our results from South Asia include that women commonly experience online abuse; with marginal sub-groups reporting more abuse. Also, women are stigmatized for receiving abuse and limit their use of platforms to protect themselves. Notable differences in our research include our sample of primarily new technology users who cope through simple technology strategies (*e.g.*, more likely to change their profile photo than update privacy settings as observed in Western populations); a higher prevalence of the three abuse types (*e.g.*, 14% content leakages among our participants over 2% in the U.S.); differences in what is defined as abusive (*e.g.*, fully-clothed photos were threatening in South Asia whereas nude photos were reported in the West); and a heavy reliance on informal support from family (over in-app reporting and legal and police recourse as noted in related work).

Abuse in South Asia

Gender-based spousal and domestic abuse is well documented in India, Pakistan, and Bangladesh (*e.g.*, [50, 62, 76, 102]). Distinguishing factors in the South Asian context (as compared to the West) include the high acceptability of domestic violence within certain limits and a dearth of institutional support for women [62]. Across various studies, it is observed that rather than surrendering to abuse, women establish a range of coping and resistance mechanisms, cognizant of their social and structural limitations [50, 53, 63, 76, 102]. Most often, women seek help from parents [62, 102]. In intergenerational families, in-laws are approached for serious violence [102]. In rural areas and urban slums, neighbors may intervene during times of violence, due to proximity [62]. Women rarely approach formal options (such as the police and shelters) due to patriarchal attitudes and difficulty in accessing the services [102]. Leaving a relationship or seeking a safe shelter is rare, although higher financial status and strong family support can motivate women to leave [48, 53, 62, 102].

Another stream of related work is on gender-based public safety concerns in South Asia (*e.g.*,[9, 20, 51]). A common theme is that women regularly use technology to feel safe in public spaces, such as by taking photos of vehicles and accessing their social networks [20, 51]. Another theme across this research is that the police are trusted for public safety like crime, but not for personal safety [20, 51], resulting in low use of SOS helplines by women [9, 51]. Prior research has examined safety attitudes of women towards digital systems, such as Bangladeshi women hesitating to use biometric systems because of male staff members and Indian transgender women finding it difficult to get Aadhar identity cards because of discriminatory attitudes of officials [8, 16, 87, 95].

Prior work touches upon online abuse in South Asia, but it is not the focus of inquiry. For example, urban Indian women had impersonation concerns when providing their phone numbers to log in to public Wi-Fi [82]. Civil society groups in India, Pakistan, and Bangladesh report that cyberlaw is inadequate and the police are not well equipped to fight online threats [1, 4, 54]. Institutional support like women's shelters are scarce and sometimes rapes occur in shelters (*e.g.*,

[69]). Abuse reporting is further limited by victim blaming and abuse justification through culture and religion [4].

South Asian feminism

Our analysis is shaped by South Asian feminist perspectives, recognizing the cultural explanations and local practices at play with technology. While South Asia has pluralistic realities, India, Pakistan, and Bangladesh have had great feminist solidarity, in part because they all belonged to an undivided India before 1947 and share a strong history of cultural interchange, trade, and family connections [28, 56, 63, 79, 88]. A South Asian feminist stance allows us to examine marginalized communities as encountering and subverting forces of power. It allows us to locate such acts in regional specificities of family, class, sexuality, and religion. South Asian feminism is often produced within the auspices of postcolonial feminism—a critique of the dominant Western feminism that saw non-white women of the Global South as powerless victims that needed rescuing or viewed gender as a universal category not intersecting with other factors [23, 64]. Feminism in South Asia moved from social reform movements for basic rights in the 19th century; to postcolonial feminism after 1940's dealing with dowry, women's work, land rights, political participation, and fundamentalism; to the present day feminism of #metoo, caste solidarity, anti-violence, anti-censorship, and LGBTQ+ rights [23, 63]—our analysis is informed by these movements, especially the struggles for equity in contemporary South Asia.

3 METHODOLOGY

Between May 2017 and January 2018, we conducted semi-structured, in-person interviews and focus groups with a total of 199 cisgender and non-cisgender members from India, Pakistan, and Bangladesh[1]. Of the entire sample, 2 participants self-identified as lesbian, 6 as queer, 3 as transgender male-to-female members, and rest were cis-gender members often in heterosexual relationships. We conducted 58 focus groups and 25 interviews with participants. We also interviewed 6 non-governmental organization (NGO) staff members (founders, managers, and crisis helpline leads) for two hours each in four women's safety and LGBTQ+ NGOs tackling online abuse in South Asia. We included NGO staff members to understand support systems and abuse experiences that might otherwise not be reported by participants due to fear, stigma, or their association with criminal activity.

Focus groups each included three participants who knew each other, such as co-workers or neighbors, to facilitate easier rapport and trust based on their common ground (see 'limitations'). Each session focused on participant's aspirations, Internet use, and safety concerns, lasting about 2 hours each. Safety-related questions were semi-structured, focusing on experiences with, reactions to, and impacts of abuse. For participants who preferred to speak alone, we conducted one-on-one interviews using the same questions.

All ten researchers share diverse ethnicities, birth countries, religions, and sexualities, but share political solidarity on feminism and technology design within which we locate this research. Most of us come from privileged positions of class and/or caste. All authors have been committed to researching gender, power, or counter-abuse in our work. The first author constructed the research approach and first three authors moderated in India, Pakistan, and Bangladesh respectively, as native researchers and regional experts. All authors were involved in data analysis and reporting.

Participant recruitment and moderation

We recruited participants through a combination of recruitment agencies, NGOs, and personal contacts, using snowball and purposive sampling that was iterative until saturation. We relied on input from regional experts when selecting incentives. We conducted interviews in local languages and translated to English during transcription in order to do comparative analysis [66] across our international team. Although we were vigilant about transcribing social, technical, and design terms verbatim, it is possible that some new etic terms may have been introduced in the translations.

We determined sample size based on ensuring representative coverage, balanced with recruitment resources available in each country. In order to obtain a well-balanced sample, we recruited participants such that roughly a third of participants each were of high, medium, and low socioeconomic status (SES) verified through income, education and material possessions [68]. Participants ranged from 18 to 65 years old. All were mobile phone owners, with 177 smart phone owners and 22 feature phone owners, with 161 prepaid subscribers. We interviewed LGBTQ+ members in India in safe NGO premises, approaching them through NGOs and activist groups[2], but did not do so in Pakistan and Bangladesh because of their high-risk safety status [46, 77]. Three-fourths of participants lived with their families, with an equal mix of nuclear families with spouse and children, nuclear families without children, and multi-generational families with with parents, relatives, and/or in-laws (most had children); one-fourth lived alone or with roommates.

[1] Our sample intentionally included heterosexual members and gender and sexual minorities. We use the term 'women' because of the broad political location of the term and the category that our participants identified with. The term does possess limitations by connoting binary biological identities and signifying the heterosexual category. We have tried to be faithful to the personal pronouns and identities used by participants themselves when we quote them.

[2] LGBTQ+ relations in India were considered illegal during the time of interviews, but were later recognized legally by the Indian supreme court in September 2018 [45].

Analysis and coding

Transcripts were coded and analyzed for patterns using an inductive approach [92]. We focused on stories about (1) access to devices and technology usage; (2) abusive incidents online; (3) abusers and perceived causes of online abuse; (4) strategies for coping with online abuse; (5) the role of formal and informal support systems in dealing with online abuse; and (6) the impacts of online abuse. From a careful reading of the transcripts, we developed categories and clustered excerpts together, conveying key themes from the data. Three team members created a code book based on the themes, with three top-level categories (types of abuse, coping practices, and consequences) and several sub-categories (*e.g.*, image distortion, abuse reporting, and reputation damage).

Numbers reported throughout the paper represent the percentage of participants who self-reported a personal abuse experience, harm, or coping practice, in a focus group or interview setting. Percentages are derived from coding each transcript for each individual's personal occurrences of abuse types, harms, and coping practices (for focus groups, each participant was coded individually). NGO participants were not included in these numbers. While we present qualitative reports of participants who reported experiences of contacts known to them to further characterize the local experience, we do not include these reports in the percentages[3].

Research ethics and anonymization

We protected participant safety, and created neutral and non-judgmental spaces, by inviting them to coffee shops, restaurants, university campuses, and NGO locations where they felt safe and comfortable. We used same-gender and same-ethnicity moderation to leverage common cultural ground and build trust. During recruitment, participants were verbally told the purpose of the study, the categories of questions, and the Google affiliation of the researchers, providing potential participants an opportunity to decline participation prior to interviews. At the beginning of each interview, the moderator obtained verbal informed consent from all participants and explained the study topics, in the language participants chose. We also informed participants that they had the right to terminate the study at any point without forfeiting the incentive. We explained the methods of recording to participants (*e.g.*, audio, video, notes, or none), after which participants chose the technique they were most comfortable with. We stored all data in a private Google Drive folder, with access limited to the research team. To protect participant identities, we deleted identifying information like names and contact details in all research files. Furthermore, we redacted any identifying information by working with privacy experts. When presenting our findings, we report only pseudonyms, age ranges, and locations (if the population is larger than 100,000 residents) to protect participant privacy; for LGBTQ+ participants, we exclude age ranges.

[3]It is possible that participants may distance themselves from abuse incidents by speaking in the third person or as a third party (see [75]).

Country-specific demographics & details

India. Our 103 participants in India included college students, housewives, domestic maids, village farm workers, IT professionals, bankers, small business owners, and teachers. We conducted focus groups in Chennai, Bangalore, Delhi, Kanpur, and villages in the state of Uttar Pradesh (an 85% urban and 15% rural split across all locations). Of this sample, 11 identified their sexual and gender identities as bi-sexual, transgender, and lesbian and 2 had disabilities. We also interviewed 4 staff from three NGOs working in women's rights and LGBTQ+ rights (2 crisis helpline leads, 1 founder and 1 manager). We identified the NGOs through Internet searches and word-of-mouth references from the LGBTQ+ community. We conducted interviews in Hindi, Tamil, Kannada, and English, depending on the participants' language preferences. Each participant received 10–15 USD for participation.

Pakistan. Our 52 participants in Pakistan included housewives, students, gym trainers, janitors, beauticians, teachers, security professionals, and home tutors. We conducted focus groups in urban and surrounding rural areas of Lahore, Multan, Rawalpindi, Peshawar, Karachi, and Hunza (an 80% urban and 20% rural split across all locations). We also interviewed 2 staff members in a women's safety NGO that provided counseling services for online abuse. We identified the NGO through word-of-mouth recommendations from some participants. We visited Muslim, Christian and Ismaili communities to recruit participants. We conducted all focus groups in Urdu. We provided participants with goody bags consisting of food items worth up to 5 USD. We also provided cash incentives worth 50 USD to facilitators in each city.

Bangladesh. Our 44 participants in Bangladesh included garment workers, housewives, teachers, medical doctors, engineers, and day laborers. We conducted focus groups in Dhaka, Chittagong, and Sylhet (all urban). We contacted participants from each group through a known contact, such as a research team member, university staff, or personal contact. We conducted focus groups in Bengali. We provided participants with incentives of warm food and monetary incentives of 12 USD, or an equivalent gift.

Limitations

Although our study included a diverse sample, it may be subject to common limitations of qualitative studies, including recall and observer bias, participant self-censorship, and limited generalizability of the results. We included percentages to indicate broad trends in our study sample of 199

women, not to generalize abuse types or reflect actual incidence rates within a broader population of South Asian women. This is particularly true as the interviews depended on what participants remembered and felt comfortable reporting in a semi-private setting (which could reduce their comfort level with speaking up, or conversely incentivize speaking among trusted contacts). Further, participants were informed beforehand and at the start of interviews about the nature of the study, and may have some level of willingness to discuss abuse-related topics. NGO staff participants discussed more abuse incidents of high severity, perhaps because of their reduced risk of stigma or trauma as compared to participants. While we attempt to highlight variations and similarity across demographics in our results presentation, future work could explicitly compare cohorts. Our study primarily reflects new technology users mainly on prepaid connections. Our numbers for LGBTQ+ (n=11) and persons with disabilities (n=2) are small, and only offer directional results, not conclusive findings.

4 FINDINGS

A majority of participants (72%) reported facing online abuse, and many narrated severe abuse incidents. Out of the remaining 28%, 7 participants explicitly reported not having faced any online abuse, and the rest did not mention any abuse incidents. South Asian women are not a singular group and these abuse experiences, impacts and resources vary across social class, age, sexual identity and community, and we attempt to underscore some of the variations. Overall, we found that participants who were younger, low-income, rural, gender minorities, or had disabilities reported greater abuse. Various factors appeared to contribute to greater abuse among these sub-groups, such as higher marginalization of minority gender identity or orientation; higher expression of violence at lower incomes (also seen in [17]); tighter nature of community living spaces in urban slums and rural areas (also seen in [85]); and higher marginalization of people with disabilities (also seen in [71]. Refer to table 2 for incidence by sub-groups. We describe the types of abuse faced by participants, the impact of the abuse on their online activities and personal lives, and the coping practices they developed to mitigate future abuse.

Types of online abuse reported

Participants primarily reported three forms of abuse: cyberstalking, impersonation, and personal content leakage. We categorized abusive behaviors according to the 'abuse type' definitions shown in Table 1, which focus on the actions abusers took and the mechanism they employed (as opposed to the abuser's motivations or victim harms, since we did not interview abusers and harms overlapped across abuses).

Cyberstalking (66%). Cyberstalking involved participants receiving constant, unwanted contact from male strangers online. Cyberstalking was the single most common form of abuse reported, with 66% discussing at least one form of cyberstalking, and 5 distinct incidents from NGOs. Younger women predominantly reported experiencing cyberstalking incidents, with some women experiencing such abuse on a daily basis; cyberstalking was more commonly reported in India (73%) compared to Pakistan (65%) and Bangladesh (50%). Participants reported receiving daily calls, friend requests, and direct messaging from unknown men (most of these were sexual in nature). Participants also described how social platforms and communication tools created new channels for connection and messaging that were leveraged by ill-intentioned strangers. As an analogy, participants described having firm control over their physical mobility and having some control over the associated risks of being out in public spaces, but because of the broader potential for interpersonal connection enabled by online social platforms, they reported being exposed to new vulnerabilities. Participants reported that they could generally ignore cyberstalking. However, when made visible to family, it sometimes led to tensions and violence, as we detail in the impacts section.

Friendship requests (55%)

Cyberstalking most commonly occured via friendship requests accompanied by 'I love you' and other sexually explicit messages from strangers. Indian participants reported higher incidence of friendship requests (67) compared to those in Pakistan (46%) and Bangladesh (36%). Platforms designed with any connection element, including mechanisms to call or direct message, were reported to lead to undesired contact. Shanti (a 25 to 30-year old from Bangalore, India) described how even non-social platforms like classifieds and marketplaces led to unwanted personal attention via their communication features.

> *"On social media platforms they say 'I love you,' 'come with me.' Everyday I get these requests. Recently I posted a scooter ad on a classifieds app, and even there I got requests, 'Do you want to have sex?' They don't leave us alone anywhere we go."*

Another form of cyberstalking involved strangers creating false profiles posing as women or trusted contacts and then sending our participants deceptive friend requests. In the South Asian context, cross-gender interactions can be problematic because of gender and safety norms. Posing as a woman was a common abuse strategy to infiltrate into individual friend lists, women-only groups, and closely-knit communities. Once abusers gained access, participants reported receiving direct messages and being tagged in content. In related cases, abusers copied the participant's photos for wider circulation (discussed later in personal content

leakages). Despite rigorous measures to protect themselves, many participants were deceived by sophisticated profiles that appeared to be authentic, through the use of common interests and relationships. In the case of Sapna (an 18 to 25-year old college student in Kanpur, India):

> *"Once I got a friend request from a girl who said we met at an arts college event. So I became friends. Then she was messaging me everyday. Then I got a suspicion that she is a he. No girl will chat so much and send hearts. Then she said 'I love you'."*

Unwanted phone calls and SMS (34%)

Cyberstalking also manifested as unwanted phone calls and SMS, with a sexual or romantic intent. Participants felt intentionally targeted due to their gender and reported that a majority of such incidents involved unknown male strangers. Mishita (a 20 to 25-year old garment factory worker in Dhaka, Bangladesh) reported how unwanted calls led to her parents suspecting her of engaging in relationships with men:

> *"I get these calls a lot. Mainly after I recharge [top-up] my phone at the shop. It's so irritating. I tell them I am married, have a baby, but still they call. My father asks me, 'who is calling you so many times, is it a man'."*

Participants believed that abusers found their contact information within and outside of technology platforms. Within platforms, participants reported that their contact information was visible to abusers via platform searches and mutual contacts. Outside of platforms, participants suspected that their phone numbers were distributed digitally through male groups, like college peer groups and neighborhood groups, and offline through top-up shops[4] (note that we describe a different abuse type in which abusers leaked content in undesired contexts under 'personal content leakages'). A few participants reported increased cyberstalking after interacting with taxi services and delivery agents. For example, Sharifa (an 18 to 25-year old college student from Karachi, Pakistan) described how taxi drivers contacted her after she used ridesharing apps.

> *"Every time I take a taxi, I get 'good morning' or 'I love you' messages. It disturbs [bothers] me."*

Impersonation (15%). Impersonation was another frequent type of abuse reported by participants, with 15% reporting at least one type of impersonation threat, and 7 distinct incidents from NGOs. Impersonation was reported more commonly in Bangladesh (34%) and Pakistan (19%), compared to India (5%). Impersonation was more commonly reported by lower-income participants, younger participants, and sexual minorities. Here, abusers would copy a victim's profile or likeness and use it to create a malicious profile or likeness, without the victim's consent. Participants discussed two common approaches: (i) stitching pornographic images to an individual's face (which we refer to as *synthetic porn*); and (ii) stealing an individual's identity to create a false, disreputable profile. Participants felt that motivations for such attacks were to humiliate women who went against dominant societal values (*e.g.,* for wearing modern clothing).

Synthetic porn (6%)

Synthetic porn involved superimposing pornographic images below women's faces. A non-trivial 6% of our participants reported experiencing synthetic porn. Threats of this type were complicated by the fact that these participants were initially unaware that their personal content was copied, manipulated, and reshared on social media platforms. For example, one participant's vacation selfie on a social platform was manipulated and spread virally, without her knowledge. None of the participants who reported experiencing a synthetic porn attack were aware of or alerted immediately afterward; rather, negative repercussions from their community made them aware that their identities had been misappropriated. In Dhaka, Saffiya (a 18 to 25-year old college student from a low-income community) recounted an incident of how a sister's display picture was superimposed onto a nude body and circulated on social media. The photo circulated on social networks for a while, before the family discovered the damage to her reputation from negative gossip within the community. For many participants, the *fear* of synthetic porn led to content censoring, such as using non-face images as profile photos (we discuss more under 'coping practices').

Stealing a victim's identity for a false profile (12%)

Twelve percent of our participants experienced impersonation attacks that involved an abuser creating a malicious or disreputable likeness of a victim's identity without the victim's knowledge. Consider the case of Mariyam (an 18 to 25-year old gym trainer in Lahore, Pakistan). When Mariyam was in the 12th grade, her profile photo and identity were exploited to create a sexually-revealing, false profile. She described that many male classmates made sexual gestures to her suddenly. Later, one of her classmates told her about the incident. Mariyam's school principal rebuked her *"loose character"* and blamed her family for raising a morally corrupt daughter. Mariyam luckily recovered from the incident by shutting down her account with family support.

Participants in Pakistan reported account hacking by strangers to maliciously modify their profiles. For example, Faiza (an 18 to 25-year old student from Peshawar, Pakistan) described how her account was misappropriated to falsely show that she was engaged to an unknown man. Fear of hacking was widespread and participants coped with this concern by carefully befriending only trusted contacts (even

[4] In 2017, the Hindustan Times reported that top-up shopkeepers were copying women customers' phone numbers and selling them in bulk packages to strangers [2].

Abuse types	Mechanisms	Harms	Coping practices
Cyberstalking (66%) Undesired contact from strangers on platforms. *IN: 73%, PK: 65%, BG: 50%*	• Friendship requests from strangers (55%) • Unwanted SMS and calls (34%)	• Self censorship and limited participation • Emotional damage • Physical violence	• Block requests • Limit information online • Use fake identities • Check for mutual trust
Impersonation (15%) Malicious likeness of a victim's identity, created or modified without consent. *IN: 5%, PK: 19%, BG: 34%*	• Synthetic porn (6%) • False profiles using a victim's identity (12%)	• Reputation damage • Emotional damage • Physical violence	• Proactively change profile photos to non-face images • Support from family and friends • Support from NGOs
Personal leakages (14%) Non-consensual exposure of interactions and content in unwanted social contexts. *IN: 7%, PK: 25%, BG: 18%*	• Non-consensual sharing of photos, conversations, and identity (14%)	• Reputation damage • Emotional damage • Coercive romantic involvement • Physical violence	• Support from family and friends • Support from NGOs • Support from police

Table 1: Threat model of online abuse types, harms, and coping methods among participants in South Asia (percentages exclude NGO staff). Participant reports are likely to be low estimates, because of the stigma and trauma of discussing abuse. Among only 6 NGO staff interviews, we heard an additional 15 distinct incidents (5 cyberstalking, 7 impersonation, 3 leakages).

though account passwords can technically be hacked by anyone), which we describe later under 'coping practices'.

Personal content leakages (14%). Personal content leakages were the final type of abuse from our study, and the most severe threat. Leakages involved abusers non-consensually leaking interactions they had with the participant or the participant's content to other individuals, with the reported goal of causing the participant harm (reported by 14% of participants, and 3 distinct incidents from NGOs). Leakages were more commonly reported by sexual minorities and low-income participants; and by participants in Pakistan (25%) and Bangladesh (18%), compared to India (7%). Participants had control when producing and sharing the content in the original context, but abusers surprised participants by releasing the content into new social contexts in malicious ways. Abusers turned ordinary interactions, such as friendly chats and normally innocent photos, into harmful content by leaking it in unwanted contexts, such as to her elderly relatives, employers, or to the public. For example, a participant who messaged with a man she did not know well was framed as licentious and evidence of the interaction was used as blackmail. Content leakage abusers were sometimes strangers and sometimes former acquaintances, acting after their interactions with the participant soured (in contrast to impersonation attackers, who participants described as strangers manipulating innocuous content).

Abusers were reported to coerce some participants into non-consensual romantic relations by threatening to leak personal content like phone numbers, names, photos, and screenshots of casual conversations. For example, Chandra (a 25 to 30-year old in Delhi, India) described threats received from a male stranger saying, *"talk to me every day or I will tell your family that you were talking to me."* As we mention earlier, cross-gender interactions were generally considered taboo among conservative families. In another case of non-consensual data disclosure, Sakshi (from Chittagong, Bangladesh) reported that her 18 to 25-year old relative's fully-clothed modelling photos meant for private publication unknown to family (as a side job), were almost leaked by a stranger who threatened to post them on social media unless she would be intimate with him. The abuser had created a page named *Shikto Noyon* (Wet Eyes) and posted that *"interesting photos will come soon"*. The link was shared with Sakshi's relative, who ultimately sought an NGO's help.

In addition to leaking conversations and images of participants, photos of women going about their daily lives were reported to be surreptitiously captured and used to cause harm. Nur (a 30 to 35-year old faculty) reported how some male students took photos of women in the college canteen, anonymously uploading them to various websites with captions like, *"how much for her?"* (implying that they were sex workers). The websites were taken down and re-created on servers in other countries. Nur noted that the women students were blamed by other faculty for exposing themselves, leading to further unwillingness by students to report abuse.

Personal content leakages were the most incapacitating class of abuse in our study, principally due to the damage they caused to participants' social reputation and dignity. Participants described how reputation damage was rooted in the suspicion of a woman's presumed complicity and looseness in leaking sexual content about themselves, even when the release was non-consensual (due to presumed sexual and premarital relations, considered taboo for most women). Content that is not (or only mildly) sensitive in Western contexts was sometimes very sensitive to the women in our study—a fully-clothed photo or a woman's name, when revealed in the wrong context, led to enormous negative consequences for women (in contrast to sexually explicit images and acts being held against women in Western contexts [99]). As Raheela (NGO staff for a women's safety helpline in Pakistan), explained,

> *"Sharing a girl's picture may not be a big deal for U.S. people, but a fully-clothed photo can lead to suicide here in conservative regions of Pakistan."*

Sub-groups	Reported at least one type
18-25 y.o.	78%
26-40 y.o.	67%
41+ y.o.	61%
Low	76%
Mid	70%
High	50%
City	73%
Town	50%
Rural	80%
LGBTQ+	100%
Persons with disabilities	100%

Table 2: Sub-groups reporting at least one abuse type.

Impacts of online abuse on participants

Although we did not specifically sample for victims of abuse, our participants experienced online abuse frequently and the impacts were severe. In this section, we discuss the repercussions of abuse, ordered by reports of how many participants experienced them (refer to Table 1).

Emotional harm and withdrawal (55%). Participants reported that all three abuse types made them uncomfortable with expressing their personal identities online and offline. Stigmatization from online abuse was especially encountered in close-knit (offline) communities via hurtful discussions at weddings, festival celebrations, and gatherings. This caused participants to withdraw inwardly, away from their communities. Two transgender participants described how online abuse made them feel more other-ed in their community and even led to self-loathing. Describing the impact of the false profile created of her, Mariyam (a cis-gender participant whose story can be found in the section about 'false profiles' above) noted how she was subjected to ridicule by her neighbors, despite her family's staunch support.

> *"I was feeling so guilty. I felt that every neighbor was laughing at me and started wondering what he has seen about me. It was terrifying."*

Online abuse (and its anticipation) led to withdrawal from activities and expression online, too. Participants reported self-censorship of their online self-expression (*e.g.*, limited profile information), reduced content production (*e.g.*, hesitation to create posts and articles), and limited content engagement (*e.g.*, refraining from commenting), to protect themselves from the antagonistic behaviors. We observed that participants were more comfortable with consuming and sharing content, than with creating content. Women-only and closed discussion groups were favored due to a sense of control and trust. Some participants expressed strong hesitation in disclosing phone numbers, names, gender, and location, which are basic units of many digital profiles.

Reputation damage (43%). A major consequence of online abuse was that of reputation damage of the self, family, and community. Distinct from the literature in the West, abuse experienced by our participants impacted not just the individual's personal reputation, but also their family and community's image and honor. Impacts included adverse social gossip, loss of arranged marriage opportunities, and rejection from parent-teacher meetings. In the case of employer leakages, managers were reported to discretely handle the situations by confronting abusers or admonishing the victim for leaking content—institutional counselling was either unavailable or not sought out. Shazia (NGO staff in Lahore) explained how the underpinning threat of reputation damage gave power to the abuser:

> *"Most threats are, 'I will put this online and show your father', not money. If the patriarchal society does not react then a blackmailer has no power."*

Coercive romantic involvement (5%). Our results show the pervasiveness of strangers attempting romantic contact with participants. Five percent of participants gave in to coercive romantic relations due to threats, mainly from content leakages (3 had ongoing relations at the time of interviews). They did not seek external help, but instead waited for the abuser to stop contact. Participants reported that the normalization of stalking in regional films provided men with frameworks for non-consensual relations.

Participants from marginal communities, such as LGBTQ+ members and women with disabilities reported facing regular

threats of coercive sexual or romantic involvement, and gave in to some of them. For example, a trans woman in India reported that she was threatened by strangers about leaking her photos along with her gender identity on social media, in exchange for sexual relations. As she had not yet publicly transitioned and LGBTQ+ relations were criminalized, she gave in to the demands for fear of losing her professional job, until she found an NGO to help file a police complaint. Participants feared potential arrest and loss of livelihood due to gender identity leaks. Participants with disabilities reported facing pervasive discrimination and vulnerability, sometimes even receiving coercive sexual threats. Through photo leaks and offensive comments that explicitly shamed disabilities, abusers made efforts to coerce relations.

Physical harm (4%). Four percent of participants reported experiencing physical violence as a consequence of online abuse, not just from intimate partners, but also from brothers and uncles who found out about the incidents. Violence was reported by 8 participants, all of whom were of lower SES (class-related reporting bias may impact middle and upper classes from disclosing violence too). Families also banished them from using the Internet temporarily and had them delete accounts. Domestic violence was reported to occur in response to all three types of online abuse.

Coping practices to deal with online abuse

To resolve online abuse, participants often sought support from family and friends, but rarely turned to online platforms or law enforcement for support. Participants attempted to prevent online abuse through technology, for example, using non-face profile photos or checking profile attributes before befriending contacts. A few participants described how they provided emotional or technical support to other contacts who went through abusive experiences, based on their prior experience. See Table 1 for more.

Resolving online abuse through informal support.

Support from family and friends (47%)

Family and friends were the most common support systems for our participants when resolving online abuse. These trusted relations offered emotional support, confidentiality, and technical advice for how to resolve or avoid abuse. For example, Saffiya's family (after the synthetic porn incident) directly confronted the abuser who lived in the neighborhood, instead of filing a police complaint, a non-bailable offense, to avoid further retaliation. After Mariyam's impersonation incident, her family provided emotional support and dealt with school authorities. Faiza (whose profile was hacked and modified) had an aunt who helped her cope with the false fiancé profile and kept the incident hidden from her strict parents. While most participants described their families as being supportive in combating online abuse, there were a few cases of domestic violence from abuse (see also Qandeel Baloch and Vinupriya's cases [39, 67].)

Appealing to NGOs (7%) and the police (1%)

NGOs provided support to 7% of our participants. These participants described NGOs as offering harassment-free support, confidential from husbands and in-laws. NGOs had vast amounts of experience dealing with online abuse cases and working with legal systems, especially for marginalized communities. However, NGOs appeared to suffer from poor discovery—a majority of participants were not aware that they could turn to NGOs for help with online abuse or did not know which NGOs to contact.

None of the women in our study approached law enforcement on their own for help with online abuse (only 1% reported to police, and these were with help from NGOs). Participants described law enforcement as being abusers themselves, bringing disrepute to women, and having outdated technical knowledge. Moreover, participants described the cybercrime reporting process as harrowing and bureaucratic. For example, the NGO staff we interviewed in India and Pakistan described the reporting process as vague (*e.g.*, it was unclear which documents to complete and what type of complaints to file). A Pakistani NGO staff member described their experience with attaching evidence to a police report:

> *"To register a complaint you must bring the printouts or photos. So for a nude photo for which someone is blackmailing me, I have to give the printout to the investigation officer. Now that file can be placed on any desk or cupboard and seen by any officer as per his convenience."*

Reporting abuse to platforms (2%)

In-app abuse reporting is a common functionality on social platforms for users to submit abuse incidents; however, only 2% of participants had reported abuse to technology platforms (half of these were from NGOs). Barriers to reporting included poor awareness of reporting features and a perception that social platforms would not understand regional problems. Relatedly, abuse reporting terms did not match the terms frequently used by our South Asian participants for the same concepts. For example, instead of using terms like 'report abuse', participants used the term 'blocking' verbally; instead of 'sexual harassment', participants used the term 'eve-teasing' (see more on privacy vernacular in South Asia in [83]). Our NGO participants who reported abuse described experiencing lengthy delays, rare take downs, and canned responses. Overall, participants described feeling that abuse reporting was not designed to help alleviate their grievances. For example, Mariyam (see Impersonation section above) did not report abuse online or flag the false profile. When

asked why in the interview, her reply was, "*What will they do anyway? I don't feel they can do much for me.*"

NGO participants believed that social platforms did not consider the South Asian cultural context when reviewing abuse complaints. For example, fully-clothed photos might not violate platform policies, even if a harasser was using it to abuse someone. Review teams' limited understanding of local languages was cited as another challenge. An NGO social worker in Peshawar, Pakistan described how a group of male college students demanded prepaid data top-ups in exchange for not leaking victims' fully-clothed photos and phone numbers on a social platform. A victim had sought the help of the NGO, following which, they reported abuse to the platform. It took a week of back-and-forth between the moderation team and the NGO to translate the page content from Pashto to English. While the page was eventually taken down, a week's delay in translation enabled further abuse.

Preventing online abuse through technology.

Establishing common trust signals (56%)

To prevent cyberstalking by strangers, participants reported checking for common ground and trust signals before communicating with new profiles, such as mutual friends, activity history, and profile content. Participants were widely aware of telltale signs of false profiles, such as profiles with women actor photos as profile photos, zero mutual connections, and one-sided posts with no engagement from contacts.

Using non-face photos (41%)

Another common practice participants employed to prevent synthetic porn or other abuses of their likeness, was to use non-face alternatives as their profile photo, such as flowers, animals, landscapes, dolls, babies, religious quotes, and family photos. Participants cared about their profile photo and thus reported conducting comprehensive image searches to find creative image alternatives. Some married women considered it more socially acceptable to display their faces along with family members. In Bangladesh and Pakistan, some participants substituted faces in display pictures with alternatives in order to observe *purdah* (veiling) for modesty and religious reasons. Participants described learning these strategies from social relations like siblings, partners, and friends. Many participants noted that when they uploaded face images, their male relatives immediately warned them about the possible dangers of exposure.

Other technology practices

Participants used other technological practices to prevent and deal with abuse, such as limiting what they shared about themselves online (59%); blocking abusers (26%); ignoring abuse (25%); and using false, male identities (6%). False identities were created via male names and profile photos (obtained via Internet searches) to participate in public fora. All participants articulated a belief that limiting their online presence would help prevent undesired abuse.

5 DISCUSSION

Overall, the participants in our study reported experiencing regular online abuse and understood their online risks fairly comprehensively. Younger, rural, low-income as well as sexual minorities and women with disabilities reported more abuse. Our results show that social media provide new spaces for patriarchal control, as much as they empower, through communication features that open interactions with abusive strangers; mis-appropriations of identities through malicious likenesses; and leaks of consensual content in unintended contexts. However, our participants did not silently experience the abuse online; rather, they strategically employed a range of informal coping mechanisms, such as relying on family, employing safeguards, verifying mutual trust signals, relying on NGOs, and reducing their online presence. In line with South Asian feminists, we echo that such acts of agency and repair need to be embraced in any interventions [62, 76].

Online abuse can have profoundly disparate impacts [25] on gender equity online in the short- and long-term. As data-driven technologies like artificial intelligence and machine learning proliferate, online abuse directly contributes to gender gaps online [42], which in turn causes gender disparity in data sets in training and evaluation, leading to fairness and ethical issues (for example, only 29% of Internet users in India are women, leading to over-representation of male data relative to their real world prevalence [84]). Addressing online safety is a starting point to an equitable Internet for women and LGBTQ+ members to connect and demand accountability. Given the complex social, cultural, and technical issues our study highlights, we argue that a coordinated, multi-disciplinary set of solutions need to be explored, encompassing design, policy, and more. We discuss some implications from our research below.

Solutions to address gender-related online abuse in the South Asian context need to consider familial and sociocultural power relations. Participants turned to family for emotional and material support to recover from abuse, although they were not unanimously helpful. Considering that the onus of a family's and community's reputation often rested on women, the prevalence and consequences of abuse were compounded for them. However, unlike domestic abuse and public harassment, older generations are excluded from understanding and handling the online threats due to their limited digital capabilities[5]. Younger male family members performed important care work and enacted 'supportive masculinity' [24], *e.g.*, by encouraging their sisters to modify

[5]Note that in South Asia, the Internet is dominated by young men, *e.g.*, [18]

their profile photos to avoid potential abuse online. Such actions protect the individuals involved from abuse, but also reinforce familiar patriarchal norms by limiting online presence based on gender. Furthermore, the public manifestation and viral diffusion of social media-based abuse present new challenges for secrecy (who can see), accountability (who is at fault), and recovery (what can be done), unlike other forms of discrete abuse which families can understand how to deal with. Support options are still entrenched in the socializing forces that endorse and lead to abuse—shifting the mindset of how gender is viewed in the family and community is important. Educating young Internet users about how to equitably and respectfully interact with women online can be effective, rather than calling for women alone to claim online spaces. Internet safety education aimed at families can be especially beneficial in the South Asian context.

Formal support systems, like abuse laws and content policies, were viewed as less supportive of gender-based abuse. Most participants perceived law-and-order and in-app abuse reporting to be ineffective or hurtful to their reputations. Only 1% had reported online abuse to police and 2% reported to platforms (compared to 27% among Western participants in [55]). Among those that had filed police complaints, paper evidence and victim-blaming were seen as detrimental to seeking help. Counter-abuse policies and moderation on technology platforms were viewed as culturally incongruous. For example, a fully-clothed photo, name, or phone number released publicly was a serious issue for some participants when deemed harmless by the platform. As another example, many participants were not aware when their digital identities were impersonated until they felt the repercussions, as in Mariyam's impersonation and the Dhaka college incident. Such events caused major damage hyper-locally because of the tight-knit nature of communities; but counter-abuse systems may only trigger when attacks happen on a large scale. Automatic detection and timely responses could help sooner. Overall, more sensitive formal recourse, technological safeguards, and improved in-app abuse handling could help South Asian women feel safer online.

NGOs acted as alternatives to formal systems by helping victims navigate legal processes and get relevant resources; however, they faced discovery issues. Future research could explore tightly coupling NGOs with formal support systems to recognize digital abuse patterns and provide support when needed. Some key questions are whether and how NGOs can handle the resulting volume of reports and how they can play a larger role in helping platforms with language translation and cultural explanations in their moderation. For example, NGO staff felt that abuse content in South Asian contexts was not well understood by social platform moderation teams, and they played critical bridges between communities and platforms, like in the Peshawar top-up blackmail incident. Another opportunity is to improve the visibility of gender equity NGOs within communities, police, and platforms.

We encourage technologists to explore user education around safety features and to set defaults that take regional specificities into account. Although technological strategies were used by participants, these were sometimes ineffective in addressing the root causes (*e.g.*, blocking contacts instead of modifying privacy settings). It is also important to offer flexibility in user identity models without impinging on users' freedom of expression. For example, participants regularly employed non-face content for profile photos, such as babies or flowers, to both prevent distortion and to enact cultural and religious values. Understanding and designing with local technology vernacular could make tools more inclusive. Our participants also sought out safe spaces, like same-gender groups, and were more likely to use them than open public platforms (similar to veils that provide 'portable seclusion' [7, 72]). While same-gender spaces may segregate women's contributions from the Internet ecosystem, design principles from these, such as moderation and reinforcement of community guidelines can help.

6 CONCLUSION

We presented a qualitative study of online safety among 199 cisgender and non-cisgender people who identified as women and 6 NGO staff members, across a diverse socioeconomic spectrum in India, Pakistan, and Bangladesh. We described the types of online abuse that South Asian women encountered and coped with, analyzing their unique sociocultural contexts and technology use-cases, using a feminist lens. We presented three major abuse types experienced by our participants, primarily on social media platforms: (i) cyberstalking, (ii) impersonation, and (iii) personal content leakages. Our results show that online abuse was commonly experienced by our participants (72% experienced at least one abuse type) and created severe consequences such as reputation harm, emotional harm, coercive relations, and physical harm. Our participants had developed informal coping mechanisms to resolve abuse, relying on family and NGOs, rather than seeking formal support from law enforcement or technology platforms. To prevent abuse, participants proactively limited technology use and used creative workarounds, leading to even lower participation online by women in a region with the highest gender gaps online [41]. Given these results, we discussed opportunities, open questions, and challenges for technologists and policy makers to consider in advancing a gender-equitable Internet .

7 ACKNOWLEDGEMENTS

Our sincere thanks to our participants for letting us into their lives, and our NGO and research partners for enabling this access. We thank our CHI ACs and reviewers, Jose Manuel

Faleiro, Patrick Gage Kelley, Daniel Russell, and Lawrence You for their helpful feedback. We thank Cheng Wang for his quantitative expertise and the following collaborators for research contributions: Garen Checkley, Taylor Marable, Oxana Comanescu, Silvia Ahmed, Tallal Ahmed, Chetna, Beenish Fatima, Maham Javaid, Muhammad Salman Khalid, Syeda Khan, Tanvir Mushfique, Shahreen Psyeche, Rahath, Rahat Jahangir Rony, Zaheer Sarwar, Syeda Aimen Shah, and Sarah Shoilee.

REFERENCES

[1] 2017. *Hamara Internet: Measuring Pakistani women's experiences of online violence.* Technical Report.
[2] 2017. *Hindustan Times: Stalkers' delight: Mobile numbers of girls for sale in UP recharge shops.* https://goo.gl/bfVEDk
[3] 2017. How 'Doxxing' Became a Mainstream Tool in the Culture Wars - The New York Times. https://www.nytimes.com/2017/08/30/technology/doxxing-protests.html. (Accessed on 09/15/2018).
[4] 2017. Legal action on cyber violence against women. (12 2017).
[5] 2018. Definitions - Cyber Civil Rights Initiative. https://www.cybercivilrights.org/definitions/. (Accessed on 09/15/2018).
[6] 2018. Sexual Harassment. https://www.eeoc.gov/laws/types/sexual_harassment.cfm
[7] Lila Abu-Lughod. 2002. Do Muslim women really need saving? Anthropological reflections on cultural relativism and its others. *American anthropologist* 104, 3 (2002), 783–790.
[8] Syed Ishtiaque Ahmed, Md Romael Haque, Shion Guha, Md Rashidujjaman Rifat, and Nicola Dell. 2017. Privacy, security, and surveillance in the Global South: A study of biometric mobile SIM registration in Bangladesh. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 906–918.
[9] Syed Ishtiaque Ahmed, Steven J Jackson, Nova Ahmed, Hasan Shahid Ferdous, Md Rashidujjaman Rifat, ASM Rizvi, Shamir Ahmed, and Rifat Sabbir Mansur. 2014. Protibadi: A platform for fighting sexual harassment in urban Bangladesh. *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, 2695–2704.
[10] Chang Ailsa. 2017. Familiar-Looking Numbers Are The Latest Twist In Robocalls. *NPR* (2017).
[11] Eileen M Alexy, Ann W Burgess, Timothy Baker, and Shirley A Smoyak. 2005. Perceptions of cyberstalking among college students. *Brief treatment and crisis intervention* 5, 3 (2005), 279.
[12] Ferenak Amidi. 2018. Giving Social Media in Iran and Afghanistan a More Gender Balanced Voice. https://www.youtube.com/watch?v=BwhdA6Q1xQE
[13] Dascalescu Ana. 2018. Doxxing Can Ruin Your life. Here's How (You Can Avoid It) . *Heimdal security* (2018).
[14] Nazanin Andalibi, Oliver L Haimson, Munmun De Choudhury, and Andrea Forte. 2016. Understanding social media disclosures of sexual abuse through the lenses of support seeking and anonymity. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 3906–3918.
[15] John Ashcroft. 2001. Stalking and domestic violence: A report to Congress. *No. NCJ 186157, Washington, DC: U.S. Department of Justice* 13 (2001).
[16] Sethi Ashpreet. 2012. Getting Aadhaar card big challenge for transgenders | Deccan Herald. https://www.deccanherald.com/content/250353/getting-aadhaar-card-big-challenge.html. (Accessed on 09/17/2018).
[17] Shreya Bhandari and Jennifer C Hughes. 2017. Lived Experiences of Women Facing Domestic Violence in India. *Journal of Social Work in the Global Community* 2, 1 (2017), 2.
[18] Ananya Bhattacharya. 2018. In India, the internet is a place for urban dwellers, men and youngsters – Quartz India. https://qz.com/india/1211218/in-india-the-internet-is-a-place-for-urban-dwellers-men-and-youngsters/. (Accessed on 01/04/2019).
[19] Lindsay Blackwell, Jill P Dimond, Sarita Schoenebeck, and Cliff Lampe. 2017. Classification and Its Consequences for Online Harassment: Design Insights from HeartMob. *PACMHCI* 1, CSCW (2017), 24–1.
[20] Jan Blom, Divya Viswanathan, Mirjana Spasojevic, Janet Go, Karthik Acharya, and Robert Ahonius. 2010. Fear and the city: role of mobile services in harnessing safety and security in urban use contexts. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1841–1850.
[21] danah boyd. 2012. Truth, Lies, and 'Doxxing': The Real Moral of the Gawker/Reddit Story. *Wired* (2012).
[22] Wanda Cassidy, Margaret Jackson, and Karen N Brown. 2009. Sticks and stones can break my bones, but how can pixels hurt me? Students' experiences with cyber-bullying. *School psychology international* 30, 4 (2009), 383–402.
[23] Maitrayee Chaudhuri. 2004. Feminism in India. (2004).
[24] Radhika Chopra. 2003. Rethinking Pro-Feminism: Men, Work and Family in India. (2003).
[25] Danielle Keats Citron. 2014. *Hate crimes in cyberspace.* Harvard University Press.
[26] Danielle Keats Citron and Mary Anne Franks. 2014. Criminalizing revenge porn. *Wake Forest L. Rev.* 49 (2014), 345.
[27] Danielle J Corple. 2016. Beyond the Gender Gap: Understanding Women's Participation in Wikipedia. (2016).
[28] Chhaya Datar. 1993. The struggle against violence. *Calcutta: Stree* (1993).
[29] Jill P Dimond, Michaelanne Dye, Daphne LaRose, and Amy S Bruckman. 2013. Hollaback!: the role of storytelling online in a social movement organization. *Proceedings of the 2013 conference on Computer supported cooperative work*, 477–490.
[30] Jill P Dimond, Casey Fiesler, and Amy S Bruckman. 2011. Domestic violence and information communication technologies. *Interacting with Computers* 23, 5 (2011), 413–421.
[31] Karthik Dinakar, Birago Jones, Catherine Havasi, Henry Lieberman, and Rosalind Picard. 2012. Common sense reasoning for detection, prevention, and mitigation of cyberbullying. *ACM Transactions on Interactive Intelligent Systems (TiiS)* 2, 3 (2012), 18.
[32] David Finkelhor, Kimberly Mitchell, and Janis Wolak. [n. d.]. *Highlights of the Youth Internet Safety Survey. Juvenile Justice Fact Sheet - FS200104 (pgs. 1-2).* Technical Report. Washington, DC.
[33] Jerry Finn. 2004. A survey of online harassment at a university campus. *Journal of Interpersonal violence* 19, 4 (2004), 468–483.
[34] World Economic Forum. 2017. The Global Gender Gap Report 2017. (2017). https://www.weforum.org/reports/the-global-gender-gap-report-2017
[35] Jesse Fox and Wai Yen Tang. 2017. Women's experiences with general and sexual harassment in online video games: Rumination, organizational responsiveness, withdrawal, and coping strategies. *New Media & Society* 19, 8 (2017), 1290–1307.
[36] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital technologies and intimate partner violence: a qualitative analysis with multiple stakeholders. *PACM: Human-Computer Interaction: Computer-Supported Cooperative Work and Social Computing (CSCW) Vol* 1 (2017).
[37] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 667.
[38] FTC. 2017. Phishing. *FTC* (2017).
[39] Imran Gabol and Taser Subhani. 2016. *Qandeel Baloch murdered by brother in Multan.* Dawn. https://www.dawn.com/news/1271213
[40] Oana Goga, Giridhari Venkatadri, and Krishna P Gummadi. 2015. The doppelg'anger bot attack: Exploring identity impersonation in online social networks. In *Proceedings of the 2015 Internet Measurement Conference*. ACM, 141–153.
[41] GSMA. 2015. Bridging the gender gap: Mobile access and usage in low-and middle-income countries. (2015).
[42] GSMA. 2018. The Mobile Gender Gap Report. (2018).
[43] Debarati Halder and K Jaishankar. 2013. Revenge porn by teens in the United States and India: A socio-legal analysis. *International Annals of Criminology* 51, 1-2 (2013), 85–111.
[44] Michael James Heron, Pauline Belford, and Ayse Goker. 2014. Sexism in the circuitry: female participation in male-dominated popular computer culture. *ACM SIGCAS Computers and Society* 44, 4 (2014), 18–29.
[45] The Hindu. 2018. The Right To Love. (09 2018). https://www.thehindu.com/opinion/editorial/the-right-to-love/article24885401.ece
[46] Saroop Ijaz. 2018. *Another Transgender Woman Killed in Pakistan.* Human Rights Watch. https://www.hrw.org/news/2018/05/08/another-transgender-woman-killed-pakistan
[47] Mayank Jain. 2016. India's internet population is exploding but women are not logging in. *Scroll.in* (26 9 2016). https://scroll.in/article/816892/indias-internet-population-is-exploding-but-women-are-not-logging-inia
[48] Lakshman Jeyaseelan, Shuba Kumar, Nithya Neelakantan, Abraham Peedicayil, Rajamohanam Pillai, and Nata Duvvury. 2007. Physical spousal violence against women in India: some risk factors. *Journal of biosocial science* 39, 5 (2007), 657–670.
[49] Shagun Jhaver, Sucheta Ghoshal, Amy Bruckman, and Eric Gilbert. 2018. Online harassment and content moderation: The case of blocklists. *ACM Transactions on Computer-Human Interaction (TOCHI)* 25, 2 (2018), 12.
[50] Heidi Bart Johnston and Ruchira Tabassum Naved. 2008. Spousal violence in Bangladesh: a call for a public-health response. *Journal of health, population, and nutrition* 26, 3 (2008), 366.
[51] Naveena Karusala and Neha Kumar. 2017. Women's Safety in Public Spaces: Examining the Efficacy of Panic Buttons in New Delhi. *Proceedings of the 2017*

CHI Conference on Human Factors in Computing Systems, 3340–3351.
[52] Colleen M Koch. 2017. To Catch a Catfish: A Statutory Solution for Victims of Online Impersonation. *U. Colo. L. Rev.* 88 (2017), 233.
[53] Michael A Koenig, Rob Stephenson, Saifuddin Ahmed, Shireen J Jejeebhoy, and Jacquelyn Campbell. 2006. Individual and contextual determinants of domestic violence in North India. *American journal of public health* 96, 1 (2006), 132–138.
[54] Anja Kovacs, Richa Kaul Padte, and Shobha SV. 2013. Don't let it stand: An Exploratory Study of Women and Verbal Online Abuse in India. (4 2013).
[55] Amanda Lenhart, Michele Ybarra, Kathryn Zickuhr, and Myeshia Price-Feeney. 2016. *Online harassment, digital abuse, and cyberstalking in America.* Data and Society Research Institute.
[56] Ania Loomba and Ritty A Lukose. 2012. *South Asian Feminisms.* Duke University Press.
[57] Shadma Malik. 2017. *The spectre of online sexual harassment | The Daily Star.* The Daily Star. https://www.thedailystar.net/opinion/society/the-spectre-online-sexual-harassment-1510252
[58] Alice Marwick and Ross Miller. 2014. Online harassment, defamation, and hateful speech: A primer of the legal landscape. (2014).
[59] Christina Masden and W Keith Edwards. 2015. Understanding the role of community in online dating. *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, 535–544.
[60] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. 2017. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2189–2201.
[61] Mary Meeker. [n. d.]. 2015 Internet Trends. http://www.kpcb.com/blog/2015-internet-trends 00000.
[62] Niveditha Menon. 2008. Domestic violence in India: Identifying types of control and coping mechanisms in violent relationships. (2008).
[63] Nivedita Menon. 2015. Is Feminism about 'Women'? *Economic and Political Weekly* 50, 17 (2015), 37–44.
[64] Chandra Talpade Mohanty. 1988. Under Western eyes: Feminist scholarship and colonial discourses. *Feminist review* 30 (1988), 61–88.
[65] Ellen Nakashima. 2007. Sexual Threats Stifle Some Female Bloggers. *Washington Post* (30 4 2007).
[66] Bonnie Nardi, Ravi Vatrapu, and Torkil Clemmensen. 2011. Comparative informatics. *interactions* 18, 2 (2011), 28–33.
[67] Express news service. 2016. Girl commits suicide after morphed pics appear on Facebook. (2016). http://www.newindianexpress.com/states/tamil$_n$adu/Girl-commits-suicide-after-morphed-pics-appear-on-Facebook/2016/06/28/article3503206.ece
[68] Market Research Society of India. 2011. The New SEC system. (5 2011). http://mruc.net/uploads/posts/b17695616c422ec8d9dadafc1c3eec26.pdf
[69] FE online. 2018. *Muzaffarpur shelter home case: Major crackdown by Bihar government - The Financial Express.* https://www.financialexpress.com/india-news/muzaffarpur-shelter-home-case-major-crackdown-by-bihar-government/1267581/
[70] Tim Owen, Wayne Noble, and Faye Christabel Speed. 2017. Silenced by Free Speech: How cyberabuse affects debate and democracy. In *New Perspectives on Cybercrime*. Springer, 159–174.
[71] Joyojeet Pal, Tawfiq Ammari, Ramaswami Mahalingam, Ana Maria Huaita Alfaro, and Meera Lakshmanan. 2013. Marginality, aspiration and accessibility in ICTD. In *Proceedings of the Sixth International Conference on Information and Communication Technologies and Development: Full Papers-Volume 1*. ACM, 68–78.
[72] Hanna Papanek. 1971. Purdah in Pakistan: seclusion and modern occupations for women. *Journal of Marriage and the Family* (1971), 517–530.
[73] Justin W Patchin and Sameer Hinduja. 2006. Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth violence and juvenile justice* 4, 2 (2006), 148–169.
[74] Jessica A Pater, Moon K Kim, Elizabeth D Mynatt, and Casey Fiesler. 2016. Characterizations of online harassment: Comparing policies across social media platforms. *Proceedings of the 19th International Conference on Supporting Group Work*, 369–374.
[75] JW Pennebaker. 2011. The secret life of pronouns: How our words reflect who we are. *New York, NY: Bloomsbury* (2011).
[76] Fauzia Rabbani, F Qureshi, and Narjis Rizvi. 2008. Perspectives on domestic violence: case study from Karachi, Pakistan. (2008).
[77] Raad Rahman. 2017. *No Country for Bangladesh's Gay Men.* New York Times. https://www.nytimes.com/2017/06/30/opinion/bangladesh-lgbt-gay.html
[78] Lee Rainie. 2017. PEW survey: Online harassment. (2017).
[79] Srila Roy. 2012. *New south Asian feminisms: Paradoxes and possibilities.* Zed Books Ltd.
[80] Rebecca Ruiz. 2018. Deepfakes are about to make revenge porn so much worse. *Mashable* (24 6 2018). https://mashable.com/2018/06/24/deepfakes-revenge-porn-domestic-violence/#KSN0cUpieOqc
[81] Kohn Sally. 2015. I Got Doxxed So You Don't Have To . *Daily Beast* (2015).
[82] Nithya Sambasivan, Garen Checkley, Nova Ahmed, and Amna Batool. 2017. Gender equity in technologies: considerations for design in the global south. *interactions* 25, 1 (2017), 58–61.
[83] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laurely Gaytan-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. [n. d.]. "Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. SOUPS 2018.
[84] Nithya Sambasivan and Jess Holbrook. 2018. Toward responsible AI for the next billion users. *Interactions* 26, 1 (2018), 68–71.
[85] Nithya Sambasivan, Nimmi Rangaswamy, Ed Cutrell, and Bonnie Nardi. 2009. Ubicomp4D: infrastructure and interaction for international development–the case of urban indian slums. In *Proceedings of the 11th international conference on Ubiquitous computing*. ACM, 155–164.
[86] Doug Shadel and David Dudley. 2015. *'Are You Real?' - Inside an Online Dating Scam.* AARP.
[87] Ranjit Singh and Steven J Jackson. 2017. From Margins to Seams: Imbrication, Inclusion, and Torque in the Aadhaar Identification Project. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 4776–4824.
[88] Sushma Sood. 1990. *Violence against women.* Arihant Pub.
[89] Cynthia Southworth, Jerry Finn, Shawndell Dawson, Cynthia Fraser, and Sarah Tucker. 2007. Intimate partner violence, technology, and stalking. *Violence against women* 13, 8 (2007), 842–856.
[90] Newsweek staff. 2018. Suicide spurs web regulation in North Korea. (2018). https://www.newsweek.com/suicide-spurs-web-regulation-south-korea-92485
[91] Michele Stephanie. 2015. I Was Catfished: This Is What I Decided to Do About It. *Huffington Post* (2015).
[92] David R Thomas. 2006. A general inductive approach for analyzing qualitative evaluation data. *American journal of evaluation* 27, 2 (2006), 237–246.
[93] Patricia Godeke Tjaden and Nancy Thoennes. 1998. Stalking in America: Findings from the national violence against women survey. (1998).
[94] Michael Trice. 2015. Putting GamerGate in context: how group documentation informs social media activity. *Proceedings of the 33rd Annual International Conference on the Design of Communication*, 37.
[95] Aditya Vashistha, Richard Anderson, and Shrirang Mare. 2018. Examining Security and Privacy Research in Developing Regions. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*. ACM, 25.
[96] Jessica Vitak, Kalyani Chadha, Linda Steiner, and Zahra Ashktorab. 2017. Identifying Women's Experiences With and Strategies for Mitigating Negative Effects of Online Harassment. *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 1231–1245.
[97] Laura Vitis and Fairleigh Gilmour. 2017. Dick pics on blast: A woman's resistance to online sexual harassment using humour, art and Instagram. *Crime, media, culture* 13, 3 (2017), 335–355.
[98] Nancy E Willard. 2007. *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress.* Research Press.
[99] Benjamin Wittes, Cody Poplin, Quinta Jurecic, and Clara Spera. 2016. Sextortion: Cybersecurity, teenagers, and remote sexual assault. *Center for Technology at Brookings. https://www. brookings. edu/wp-content/uploads/2016/05/sextortion1-1. pdf. Accessed* 16 (2016).
[100] Janis Wolak and David Finkelhor. 2016. Sextortion: Findings from a survey of 1,631 victims. (2016).
[101] Delanie Woodlock. 2017. The abuse of technology in domestic violence and stalking. *Violence against women* 23, 5 (2017), 584–602.
[102] Rubeena Zakar, Muhammad Zakria Zakar, and Alexander Krämer. 2012. Voices of strength and struggle: Women's coping strategies against spousal violence in Pakistan. *Journal of interpersonal violence* 27, 16 (2012), 3268–3298.