Expanding Concepts of Non-Consensual Image-Disclosure Abuse: A Study of NCIDA in Pakistan

Amna Batool
University of Michigan
Ann Arbor, USA
abatool@umich.edu

Mustafa Naseem
University of Michigan
Ann Arbor, USA
mnaseem@umich.edu

Kentaro Toyama
University of Michigan
Ann Arbor, USA
toyama@umich.edu

ABSTRACT

Non-Consensual Image-Disclosure Abuse (NCIDA) represents a subset of technology-facilitated sexual abuse where imagery and video with romantic or sexual connotations are used to control, extort, and otherwise harm victims. Despite considerable research on NCIDA, little is known about them in non-Western contexts. We investigate NCIDA in Pakistan, through interviews with victims, their relatives, and investigative officers; and observations of NCIDA cases being processed at a law enforcement agency. We find, first, that what constitutes NCIDA is much broader in Pakistan's patriarchal society, and that its effects can be more severe than in Western contexts. On every dimension – types of content, perpetrators, impact on victims, and desired response by victims – our findings suggest an expansion of the concepts associated with NCIDA. We conclude by making technical and policy-level recommendations, both to address the specific context of Pakistan, and to enable a more global conception of NCIDA.

CCS CONCEPTS

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

KEYWORDS

Non-Consensual Disclosures, Image Based Sexual Abuse, , Non-Consensual Image-Disclosure Abuse (NCIDA), Social Media Platforms, South Asia, Women, Online Harassment, Technology-Facilitated Sexual Abuse, Gender-Based Violence

ACM Reference Format:
Amna Batool, Mustafa Naseem, and Kentaro Toyama. 2024. Expanding Concepts of Non-Consensual Image-Disclosure Abuse: A Study of NCIDA in Pakistan. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3613904.3642871

1 INTRODUCTION

Of the various social ills that digital platforms have enabled, technology-facilitated sexual abuse is arguably among the most devastating for individual victims. In the West, common forms of it include revenge porn, characterized by the distribution of private, explicit images to humiliate [36, 64, 101], and cyberstalking, in which perpetrators aim to control and manipulate intimate partners through digital surveillance and harrassment [22, 23]. These offenses disproportionately target women and other marginalized groups [39] – as much as 89% of revenge porn victims, for example, are women [64]. The impact of such disclosures is painful and multifaceted, resulting in psychological distress [4, 40, 101], reputational damage [11, 44, 64, 100, 101], financial repercussions [64], and in severe cases, physical harm [35].

In this paper, we focus our attention on a particular subset of technology-facilitated sexual abuse, in which images and video with romantic or sexual connotations – and the threat of their disclosure – is used by bad actors to control, extort, and otherwise harm victims. In Western contexts, these instances have been studied as "non-consensual intimate image" (NCII) disclosure [1, 33, 34, 98] because the vast majority of such instances involve intimate imagery. But, there are indications that in some non-Western geographies, actual intimate imagery need not be involved. In Pakistan, for example, a girl was killed by male family members for having appeared in a doctored video simply sitting next to a boy – both fully clothed – that was posted to social media by a third party [94]. In another case also from Pakistan, a woman committed suicide after innocent images of her annotated with obscene content were circulated online [13].

Some research suggests that these are severe instances of a common occurrence. The handful of studies conducted in South Asia [60, 73, 91] highlight online abuse faced by South Asian women, often involving threats to expose sensitive content to their families. Content might include fully clothed profile pictures, names, phone numbers, fake social media profiles, and unsolicited sexual messages in addition to actual and fabricated explicit content. Its disclosure inflicts significant reputational harm on victims and their family members. Thus, in some contexts outside of the West, NCII appear to be part of a broader phenomenon in which non-consensual disclosure of socially sensitive images – whether explicit or not – enables a range of abuses.

In this paper, we report on our investigations in Pakistan of that broader phenomenon – which we call *non-consensual image-disclosure-based abuse* (NCIDA). The concept of NCIDA is intended to represent a subset of tech-facilitated sexual abuse that is broader than NCII (see Figure 1). Specifically, we sought to answer the following research questions:

- In what forms do NCIDA manifest within the Pakistani context?
- What are the effects of NCIDA on victims and their families?
- What remedies do victims prefer to mitigate such abuse?

CHI '24, May 11–16, 2024, Honolulu, HI, USA

ACM ISBN 979-8-4007-0330-0/24/05
https://doi.org/10.1145/3613904.3642871

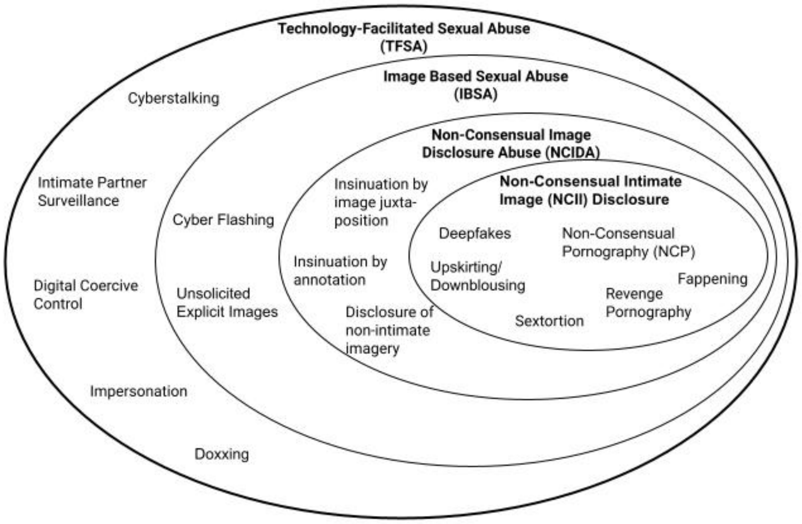
Technology-Facilitated Sexual Abuse (TFSA)
Image Based Sexual Abuse (IBSA)
Non-Consensual Image Disclosure Abuse (NCIDA)
Non-Consensual Intimate Image (NCII) Disclosure
Cyberstalking
Intimate Partner Surveillance
Digital Coercive Control
Impersonation
Doxxing
Cyber Flashing
Unsolicited Explicit Images
Insinuation by image juxta-position
Insinuation by annotation
Disclosure of non-intimate imagery
Deepfakes
Non-Consensual Pornography (NCP)
Upskirting/ Downblousing
Fappening
Revenge Pornography
Sextortion

Figure 1: Venn diagram of types of Technology-Facilitated Sexual Abuse relevant to this paper. This paper's focus – Non-Consensual Image-Disclosure Abuse (NCIDA) – falls within the broader concept of Image-Based Sexual Abuse and the narrower notion of Non-Consensual Intimate Imagery Disclosure. The diagram also includes examples of specific types of abuse that fall within each category.

To answer these questions, we collaborated with a federal law-enforcement agency and a civil society organization in Pakistan, both dedicated to women's safety online. We conducted interviews with twelve NCIDA victims, eight family members of victims, and twelve investigation officers (IOs). In addition, we conducted 240 hours of observation of investigation sessions where investigation officers spoke with the victims, their family members and perpetrators.

Our study makes the following contributions: First, we provide detailed documentation of the kinds of NCIDA that take place in Pakistan, a country that is often said to have a socially conservative, patriarchal honor culture [27, 37]. Though a handful of papers have investigated NCIDA in South Asia [60, 73, 92], our paper provides a depth of detail not previously reported. Second, our analysis confirmed a hunch we had when we began in this research – that what has been reported about NCIDA in Western contexts represents only a fraction of the types of NCIDA that occur in Pakistan in terms of image content, perpetrator types, motivations for abuse, range of victims, and impact on victims. Third and building on the second point, we argue that the previous literature is woefully skewed, centering as it does the Western experience of NCIDA while being largely oblivious of non-Western forms of NCIDA. The bias is important to highlight because it means, for example, that social-media company policies – which are often calibrated for Western users [8, 78] – may fail whole groups of victims outside the West. Based on our findings, we make user interface recommendations for technology creators, both to address the specific context of Pakistan and to mitigate a West-centric conception of NCIDA. Finally, the combination of Western and Pakistani NCIDA cases enables us to propose a preliminary NCIDA theory that suggests that NCIDA is influenced by the local culture's social and moral norms, particularly regarding romance, sexuality, marriage, and public visibility.

2 RELATED WORK

We explored the literature within the domains of HCI, legal studies, and feminist studies to understand the existing landscape of NCIDA in both Western and South Asian contexts.

As we will be making some overall claims about the existing literature, we first outline our literature-search methodology: In addition to compiling work we were previously aware of, we used Google Scholar, employing a wide range of search terms related to NCIDA, including both the spelled-out and abbreviated forms of "NCII," "IBSA," "cyber sextortion," "revenge pornography," and terms like "upskirting," "deepfakes," "downblousing," "online sexual harassment." We did not specify geography in a a systematic way, but we did look for papers addressing non-Western contexts, and specifically in South Asia, by including terms such as "Asia," "South Asia," "Pakistan," "Bangladesh," in some of our searches. This search yielded over 500 publications across various fields such as HCI, legal literature, and feminist studies. To narrow focus, we filtered out papers that only mentioned the search terms in passing, and which did not have a strong focus on NCIDA. We selected 50 papers for close review, prioritizing the typical qualities sought in papers in a literature review: seminal or foundational content, high citation count, rigorous analysis. The final list comprised 18 content analysis papers, 16 survey studies, 12 interview studies, and 4 mixed-method studies. While our literature review was not exhaustive, we believe it captures the best of the relevant work, and that it is representative of what has been written about NCIDA.

Study Location	Paper Count	Notes
US Only	27	Participants entirely within US; mix of survey and interviews.
Western Europe (Spain, UK, Belgium)	3	Participants entirely within Europe; mix of survey and content analysis.
Australia	6	Participants entirely within Australia; mix of survey, interviews, and content analysis.
Multicountry, but Anglo-centric and majority US	8	Participants from Anglo-centric regions with the majority from US; mix of interviews and content analysis.
Multicountry	3	Participants from different countries around the world (including South Asian countries: India, Pakistan) with equal representation; mix of survey and content analysis.
South Asia (India, Pakistan, Bangladesh)	3	Participants entirely within South Asia; mix of survey and interviews.
Total	**50**	

Table 1: Geographic focus of the reviewed literature, for the 50 NCIDA-related items that were reviewed. The existing literature is predominantly focused on Western contexts. (NCIDA = "non-consensual image-disclosure-based abuse")

2.1 NCIDA in Western Contexts

To begin, we note that the existing literature on NCIDA predominantly focuses on Western perspectives (47/50:~94%), as can be seen in Table 1. A summary of the reviewed literature's findings, as classified into categories we eventually used to organize our own (Section 4), is shown in Table 2.

In the Western context, research on NCIDA mainly centers on nude imagery and sexually explicit content (39/47:~83%) [21, 33, 36, 46], with prominent examples including revenge or non-consensual pornography (NCP) [47, 64, 101] and sextortion [61, 104]. For the most part, NCIDA appear to be perpetrated by current or former romantic partners [23, 33, 46] (42/47:~89%). Most victims are women [77] and other marginalized groups, such as children [61] and individuals from the LGBTQ community [41]. NCIDA is often driven by a desire for revenge [18, 46, 64, 71, 84]. This revenge-driven behavior can manifest in the defamation of victims and attempts to assert coercive romantic control [18, 30, 45, 87], especially when a victim decides to end a relationship.

Very occasionally, men are targeted [61]. In the reviewed literature, the only noted instances involve transnational criminals running online scams that seek to extort men financially [61].

The most common mechanism for abuse is either the viral dissemination of explicit content or the threat of it, to the victims' social circle or the general public through online platforms, with the aim to humiliate victims and tarnish their reputations [22, 44, 64, 76, 100, 101].

The acquisition of sensitive content can be achieved through both consensual and non-consensual means. In consensual cases, images may have been shared during the course of a romantic relationship, typically through sexting, violating trust that perpetrators later exploit to their advantage [3, 15, 19, 38, 54]. On the other hand, non-consensual acquisition often involves surreptitious gathering of images without the victims' knowledge or consent [38]. This can occur through methods such as hacking into the victim's device, physically stealing images, or coercing victims into sharing content under false pretenses through phenomenona like "coercive sexting" [24, 53, 65, 97], "fappening" (the unauthorized disclosure of a vast collection of hacked nude photographs, primarily featuring female celebrities) [51], "up-skirting" (taking pictures without consent by directing a covert camera up a female's skirt), and "downblousing" (focusing on a female's blouse to capture images of her bra, cleavage, or breasts) [17, 36, 42], among others. Additionally, technology plays a role in the non-consensual generation of explicit content, with examples like deepfakes (images or videos portraying unreal events as real through digital manipulation) [25, 31, 105].

The existing literature has also illuminated societal factors that perpetrators manipulate [6, 7, 102], such as oppression and stigmatization [41, 77, 78, 85, 102], level of tech-savviness [22], popularity [26, 51], shared proximity [6, 22], and technological anonymity [83].

As to potential remedies, the literature outlines two primary approaches: the punitive approach [29, 31, 35, 80, 103], which encompasses content removal and moderation, banning, public shaming, and criminal prosecution; and the restorative approach [22, 66, 79–81], which includes social-good-centered apologies (both public and private), voting and reward systems, legal protections, and monetary compensation. In the United States, there has been a recent shift from a punitive to a restorative justice approach; one survey finds that young adult victims prefer private apologies over public shaming (29% versus 14%) of perpetrators after instances of online harassment [81].

Legal and HCI scholars have suggested links between NCIDA and Intimate Partner Violence (IPV) [4, 16, 22, 33, 45, 63–65]. For instance, Bates highlighted that survivors of NCIDA often draw parallels between the consequences they face and those experienced by survivors of sexual assault, implying that NCIDA could be categorized as a form of sexual offense against women [4]. Some research found that adolescents involved in non-consensual sexting were significantly more likely to report dating violence and anxiety during high school compared to those engaged in consensual sexting [93]. One survey revealed that individuals experiencing cyber victimization by an intimate partner were substantially more likely to encounter in-person psychological IPV (28 times more likely), physical IPV (52 times more likely), and sexual IPV (four times more likely) [50]. And, work showing how abusers in IPV contexts exploit technologies to intimidate, threaten, monitor, impersonate, harass, or otherwise harm their victims [22] suggests that NCIDA should be seen as a digital extension of Gender-Based Violence (GBV) or Violence Against Women (VAW).

The literature summarized above is extensive, and it supplies a thorough understanding of NCIDA in Western contexts, especially as seen in Anglophone countries. It also provides a springboard for investigating NCIDA in non-Western contexts. However, as we will see in the findings, when considered as a description of what is ultimately a global phenomenon, the literature is impoverished, relying as it does on research conducted in only a few countries (see Table 1).

2.2 NCIDA in South Asia

In contrast to the extensive empirical work conducted in Western contexts, there is limited research in the South Asian context exploring technology-facilitated sexual abuse. This gap exists despite South Asia boasting one of the largest user bases of these technologies with over 961 million social media users [88].

As background, South Asian women experience multifaceted marginalization due to factors like class, literacy, religion, and cultural characteristics such as family honor, lack of agency due to patriarchy, and collectivism. This complexity is worsened by the stigma associated with connecting women's chastity to family honor [27]. Within this web of marginalization, various forms of GBV are prevalent and well-documented in South Asian communities. These include domestic violence and honor-based abuse, which includes traditional forms of abuse such as sexual assault (including within a marital relationship), honor killings, murders, suicides, dowry violence, violence in custody, marital rape, and abuse by in-laws [12, 28, 58, 59]. Structurally, patriarchal social norms, some stemming from local interpretations of religion, diminish women's status, rendering them more vulnerable to gender-based violence [28]. Culturally, some men believe that it is their right to control their wives and resort to violence if disobeyed. Women often rationalize domestic violence as a private matter, often justified by religion [28].

Prior efforts to understand NCIDA in South Asia – of which we could find only three – have examined it within the broader scope of online harassment [60, 73, 91]. These studies highlighted the online abuse of South Asian women, often at the hands of strangers who threatened to disclose victims' sensitive content to their family members [73, 91]. While this research has found instances of women's personal content leakage [73] and fabricated non-consensual pornography [91] within the realm of online harassment, they explore NCIDA only as a small part of a larger investigation of online abuse. Thus details of the rull range of NCIDAs with respect to content, perpetrator, threat mechanism, consequences, or remedies remain unknown.

Our research seeks to build upon this existing work by turning attention specifically on NCIDA in Pakistan. Our aim is to provide a thorough and detailed overview of NCIDA in Pakistan, emphasizing the distinctions between NCIDA there and those observed in Western contexts. We expect that the differences will highlight the need for culturally appropriate responses to NCIDA, and demonstrate the need for a general expansion of the conception of NCIDA among scholars.

3 METHODS

To answer our research questions, we used a qualitative approach inspired by ethnographic techniques [68], including participants observations, semi-structured interviews, and informal interactions. We spent over 300 hours in the field, involving interviews, follow-up discussions and information interactions (~60 hours total), with 12 investigation officers (IOs), 12 NCIDA victims, and 8 victim family members; and field observations (~240 hours total) of 70 official NCIDA investigative sessions, in which IOs interacted with victims, family members, and perpetrators. All fieldwork was conducted by the first author in person in Pakistan, and took place between December 2022 and August 2023. The study received ethical approval from our university's Institutional Review Board.

3.1 Study Site

Our study was conducted in a large ubran city in Pakistan, and involved collaboration with two organizations. The first is the cybercrime wing (CCW) of a federal agency that specializes in digital forensics, information system security audits, and providing psychological support to NCIDA victims. The organization employs over 2000 individuals, including female investigation officers (IOs). The second organization is a national non-governmental organization (NGO) dedicated to protecting human rights, particularly in the realm of women's digital rights. The organization has 20 employees, and provides support to NCIDA victims across Pakistan. While the NGO does not have jurisdiction to process NCIDA cases, they play a crucial role by connecting online harassment victims to a range of public services, including technical, legal, and psychological support, as well as referring them to CCW when necessary.

3.2 Participant Recruitment and Data Collection

Our participants included NCIDA victims, their family members, and investigation officers (IOs) from both organizations.

3.2.1 Semi-Structured Interviews with Investigation Officers.

We began by interviewing IOs to understand the overall landscape of NCIDA in Pakistan. We conducted 12 semi-structured interviews, with 6 female and 4 male IOs from CCW and 2 case workers from the NGO. (Given that case workers perform similar work to IOs, for the sake of simplicity, we refer to them as IOs as well in this paper.) All interviews were conducted in Urdu. Each session lasted approximately 60-90 minutes, totaling approximately 15 hours of content. The interviews covered the IO's work history, experiences working with victims and their families, types of NCIDA reported, investigation processes, interactions with perpetrators, interactions with tech companies, and lastly, responses to NCIDA that they heard from victims and the larger society. All interviews were

Dimension	**Category**	**Paper Count (W:47, SA:3)**	**Notes**
Victims' Gender	All women victims	7/50 (W:7, SA:0)	-
	Women majority, but some male and trans victims	42/50 (W:39, SA:3)	Eighteen content analysis papers report that women are victims and men are perpetrators in most cases.
	All trans victims	1/50 (W:1, SA:0)	There is growing literature on tech-facilitated abuse of the LGBTQ+ community; much of it is identity-focused but not necessarily sexual abuse.
Perpetrators	Current/former intimate partners	42/50 (W:41, SA:1)	Most common perpetrator type in the literature.
	Prospective intimate partners	9/50 (W:8, SA:1)	These are people seeking romantic involvement, or who failed in the attempt.
	Strangers	9/50 (W:6, SA:3)	These papers mention strangers sending unsolicited sexual messages and images of themselves.
	Transnational Offenders	1/50 (W:1, SA:0)	This paper identifies transnational, organized criminals who impersonate women or transgender individuals to entrap and extort men [61].
Content	Sexually explicit imagery	39/50 (W:37, SA:2)	Either actual or fabricated, sexually explicit content is the most common type of content in NCIDA.
	Non-sexual imagery (e.g., profile pictures, candid shots, etc.)	1/50 (W:0, SA:1)	One study in South Asia highlighted non-sexual content being used in an NCIDA, but specifics were not provided [73].
	Inappropriate messages, hate speech (verbal abuse)	7/50 (W:4, SA:3)	-
Threat Mechanism	Public disclosure, or threat of	49/50 (W:47, SA:2)	Most common type of threat in the literature.
	Disclosure to family members, or threat of	3/50 (W:1, SA:2)	Only 3 studies noted disclosures targeted at victim's family members, of which 2 were about South Asia, and 1 involved U.S. minors.
Consequences	For victims – emotional, physical, reputational, social	50/50 (W:47, SA:3)	All studies highlighted at least one or more of the mentioned harms experienced by victims.
	For family – reputational	7/50 (W:5, SA:2)	A few studies mentioned reputational consequences for friends and family.
Preferred Remedies	Punitive approach	19/50 (W:17, SA:2)	Content removal and moderation, banning, public shaming, criminalization, and prosecution.
	Restorative approach	9/50 (W:9, SA:0)	Apology (public and private), voting and reward system, monetary compensation.

Table 2: Summary of what the literature reviewed for this study finds about NCIDA, using dimensions for describing NCIDA that arose from this paper's analysis. (W = Western, SA = South Asian)

audio-recorded after receiving informed consent and transcribed for analysis. Participants received US$30 as a token of appreciation. Any identifiable details discussed in individual cases were scrubbed to ensure the narratives were abstracted and generalized.

3.2.2 Observations. In addition to interviews, we conducted 240 hours of observations at CCW, closely following interactions between IOs, victims, family members, and perpetrators during the investigation of 70 NCIDA cases. We took detailed handwritten notes of case-specific details such as content type, nature of disclosure, platforms used, perpetrator-victim relationship, perpetrator intent, remedies sought, family members' reactions, IO's line of questioning, victim demeanor details like body language, facial expressions, and appearance.

Given victims' vulnerable state and the sensitivity of their revelations, we went to great lengths to ensure that potential participants were thoroughly comfortable engaging as research participants. Before the start of an investigative session, the IOs introduced the first author to the victim as a research intern investigating NCIDA's impact on Pakistani victims and families. The first author then described her goals and motivation, the process of documentation (handwritten notes only; no audio recording) and analysis, and plans for publication (no individually identifiable details). Prospective participants were informed that they would be given a copy of any notes to review, that they could withdraw from the research at any point, including for at least 3 months after the session, and that participation in the research was entirely voluntary. Participants were then asked if they consented to participation in the research, and separately, to note-taking. Throughout, the first author sought to convey a tone of care and compassion, and that participants should decline if they felt the least bit uncomfortable.

Out of 78 victims who were approached, 8 declined to participate (so the first author left the room). We note, incidentally, that the investigation room in which the sessions took place was crowded with five IOs handling victims, family members, perpetrators, and office staff simultaneously. There was thus very little privacy for victims to begin with, and our observations did not affect any of the proceedings. In this setting, the additional presence of a female intern doing research was acceptable for most victims and their families.

3.2.3 Follow-up Interviews. After each session, we conducted follow-up interviews with IOs to gain deeper insights into cases. These discussions lasted about 15-20 minutes, totaling approximately 20 hours of content and were audio-recorded with the IO's consent.

As our rapport with IOs grew, they were willing to ask victims and their families if they would be open to engaging with us one-to-one. Once IOs had consent from the victim and/or a family member, to be introduced to us, they introduced us. Ultimately, 12 victims and 8 accompanying family members were willing to sit with us for individual interviews. Participants were already familiar with our consent clauses, and we reminded them of the key points. Each interview lasted 15-30 minutes, totaling approximately 5 hours of content. Due to the sensitive nature of the context and upon the IOs' recommendation, we opted not to provide compensation to victims and their family members (a similar approach was employed by Freed et al.[22] with a vulnerable population).

3.2.4 Informal Discussions. We also engaged in numerous informal discussions aimed at gaining IOs' perspective on emerging patterns in our data. These discussions took place typically on days when their caseload was lighter. Within the CCW, IOs routinely discussed various aspects of the cases among themselves, and the first author actively participated in these conversations. These discussions were audio-recorded with IOs' consent, and totalled approximately 20 hours of content.

3.3 Participant Details

We conducted interviews with 12 IOs, 12 victims, and 8 family members. As depicted in summary Table 3, among the 12 IOs, 8 were female, and 4 were male. All CCW's IOs held a range of official government positions, while 2 worked for a private NGO. Seven IO's had master's degrees in information science, 2 had dual degrees in information science and psychology, and 3 had bachelor's degrees in information science. IOs' ages ranged from 25 to 40, and they had 2 to 12 years of work experience. Table 4 shows the demographic details of the victims, including their gender, age range, marital status and occupation.

3.4 Data Analysis

We collected over 60 hours of audio recordings (including interviews (~15 hours), followup discussions (~25 hours) and informal interaction (~20 hours)) that we screened to exclude any identifiable and irrelevant information. We transcribed 50 hours of data that resulted in approximately 1,000 pages of transcripts. Additionally, we collected detailed hand-written notes taken during observations and interviews, comprises of approximately 2500 pages of notes. We conducted an inductive thematic analysis approach for data analysis [9, 10, 89]. Given the scattered nature of the data for each case, we began by composing detailed summaries for all 70 cases, compiling information from transcripts and notes representing IOs, victims, and their families. Anonymity was strictly maintained by excluding any identifiable details, ensuring abstract summaries. The first round of open coding [10] generated about 80 codes, covering various aspects like types of content, disclosure nature, technology mediums, victim categories, perpetrator types, etc. These codes were iteratively refined and clustered into categories including perpetrator types and intentions, content mining strategies, and stages of disclosure with associated technology tactics. This round of analysis yielded both novel findings and findings similar to those found in prior literature. As we filtered out redundant themes already discussed in the previous literature, we identified five key themes that are elaborated upon in our findings. While the initial coding was performed by the first author, collaborative discussions among all authors refined and structured the codes into higher and lower levels across multiple iterations.

3.5 Positionality Statement

The lead researcher, a cis-gendered, straight Pakistani woman, has extensive experience with research within Pakistan focused on online abuse of women. She has deep understanding of victims' experiences and sensitivity to their realities. At the same time, her educational status at a university outside of Pakistan, upper-middle-class upbringing, and endorsement as a researcher from senior government officials grant her privilege that contributes to power dynamics with research participants. These dynamics are impossible to eliminate, but she is aware of them and works to minimize any negative impact, including any felt pressure for prospective participants to engage in research. The other two authors are both cis-gendered men. Neither had direct contact with any of the participants. One of the male authors is of Pakistani origin, speaks Urdu, and has worked closely with Pakistani government institutions. All three authors come from non-Western backgrounds, and have contributed to multiple studies of online abuse and other topics in Pakistan.

4 FINDINGS

Trigger warning: Our findings involve discussions of topics such as violence against women, domestic abuse, suicide, and tragic deaths.

Our research uncovered a deeply troubling set of details about the nature of NCIDA in Pakistan. Many of our findings track very closely with what has been found about NCIDA in Western countries as noted in Section 2.1 (refer also to Table 2). For example, revenge porn and attempts to control romantic/sexual partners through threats of intimate image disclosure appear common, together comprising nearly a half of the cases we heard about. In many cases, the consequences for victims also tracked closely with

Gender	Age Range (Years)	Qualification	Job Role	Job Experience (Years)
Female: 8	Min: 25	MS in IT/CS: 7	Sub-Inspector: 7	Min: 2
Male: 4	Max: 45	BS in IT/CS: 3	Forensic Officer: 3	Max: 12
		MS in Psych: 2	Admin: 2	

Table 3: Demographic details of Investigation Officers (IOs) with qualifications in MS (Masters), BS (Bachelors), IT (Information Technology), and CS (Computer Science). Sub-inspectors conduct thorough investigations and prepare reports, Forensic officers handle digital device investigations and technical reports, while Admins manage cases at an organizational level.

Gender	Age Range (years)	Martital Status	Occupation
Female: 58	Min: 20	Married/Engaged: 32	Working: 18
Male: 12	Max: 65	Unmarried: 27	Student: 19
	Average: 25-35	Divorced: 10	Homemaker: 33
		Widow: 1	

Table 4: Summary of Demographic Details of 70 NCIDA Victims (including the details of 12 victims we interviewed)

what has been reported, with victims reporting emotional distress and reputational harm.

But, our study also reveals extensive new findings that go considerably beyond what has been previously reported. In organizing these findings, we found it analytically useful to bring out the contrast with existing West-centric findings. In doing this, our intention is not to center a Western perspective. Our hope, rather, is to demonstrate the dramatic difference between Pakistan and Western countries with respect to NCIDA, which will lead naturally to one of our conclusions that NCIDA research thus far has been remiss in offering a global perspective (see Discussion).

Within these findings, we identified five key dimensions of differentiation: the nature of the content, types and perpetrator motivations; threat mechanisms; impact of NCIDAs; and finally, preferred remedies. The findings below are reported in corresponding subsections.

Note on the exposition: Both for reasons of added confidentiality and the absence of audio recordings, we deviate slightly from common practice in qualitative HCI: Reports of participant utterances and scenarios that compile information gathered in one investigative session are written to bring out their essence, without attempting to capture verbatim quotes. Concrete details have been omitted, and names have been replaced with pseudonyms. Paraphrased quotations are represented in [square brackets]. On occasions where real quotes occur, they have been used with the express consent of the individuals involved.

4.1 Nature of Content

While NCIDA in prior work typically revolve around explicit imagery or sexual acts [21, 33, 36, 46, 61], our research identified (a) a significantly lower bar for what constitutes NCIDA in Pakistan, and (b) commonplace use of minor digital manipulation to make innocuous images appear sensitive, and subsequently used as NCIDA fodder.

4.1.1 A Lower Bar for Problematic Content. We found that content that may be perceived as commonplace in Western cultures – public displays of affection such as two individuals holding hands, hugging or giggling – was considered sensitive by our participants. A fifth of our NCIDA cases (14 out of 70) involved imagery with no explicitly sexual content, involving scenes such as a couple sitting together, holding hands, giving a high-five, hugging, or sharing a laugh. In using such images, perpetrators are insinuating a sexual relationship even if none existed – an insinuation that parts of the surrounding society are ready to accept. Take the case of Alishba, where the perpetrator happens to be an ex-boyfriend as well as her sister's brother-in-law. An IO reported:

> [From the time that they were dating, the perpetrator had access to a few selfies where he and Alishba were seen hugging or holding hands in public places such as parks. However, Alishba is now engaged to another person and the perpetrator is exploiting this content to coerce her family into arranging Alishba's marriage with him.]

While most victims of this content exploitation were women, in some cases men were threatened as well. Wahid's professional rivals filmed him enjoying a light moment sitting next to a *hijra* (third gender)[1] colleague during a work event. The perpetrators falsely depicted this as a marriage ceremony on social media. While explaining the content of social media in a followup interview, Wahid (the victim) reported:

> *"Look, our so-called Muslim brother [Wahid] is marrying a hijra person, which is prohibited in Islam... Should he be punished, and what is the punishment for this in Islam?"*

As a result of this post, Wahid received death threats from online extremists as well as from members within his Pashtun community, a community that is governed by a strict, patriarchal honor code called 'Nang' [43].

Apart from images of apparent couples, images of women wearing clothing that would be considered problematic by some conservative Pakistani standards was also used in NCIDA. In one example,

[1] "Hijra" and "third gender" are terms used in South Asia to describe a certain subgroup of men who cross-dress as women [70].

an IO reported that a perpetrator obtained the victim's images without their consent and threatened disclosure in order to demand sexual favors:

> [The perpetrator works at Aroosa's office and gained unauthorized access to her laptop and phone, obtaining personal photos of her wearing jeans and sleeveless tops that she was trying on in a shopping mall changing room.]

4.1.2 Turning Innocent Imagery into Compromising Content. We found that in some cases (24 out of 70), perpetrators resorted to manipulating everyday images of the victims, though still often taken without their knowledge. Perpetrators used simple techniques such as juxtaposing an innocuous image (e.g. the victim engaged in a normal video call) with an explicit one (e.g. the perpetrator in a sexual act). In one such instance, Ayesha fell victim to an 8-month-long blackmail ordeal, as reported by an IO:

> [Ayesha placed a video call on WhatsApp to inspect a phone she wanted to purchase from a seller she had connected with on a classified ads website. When the call connected, the person on the other end was fully naked and masturbating. In the time that it took Ayesha to comprehend what was happening and to hang up, the perpetrator had captured a screenshot of the video call. The perpetrator sent Ayesha the image where Ayesha's face is in the top right corner of the frame while he is masturbating. He demanded further explicit material, and when she didn't comply, he threatened to send the image to her husband and insinuate that they were having phone sex. Ayesha felt helpless and ended up giving in to his demands. Over the next 8 months, he subsequently demanded money (totalling 250,000 Rupees (approximately US$750).

In this instance, there was no compromising imagery whatsoever of the victim – her face was the only visible element in the screenshot. However, fearing consequences as dire as divorce, Ayesha ended up giving him access to even more damning imagery.

Another technique that perpetrators use is to combine unrelated images to create a collage accompanied with sexting emojis such as eggplant and peach, and captions such as 'whore', 'blasphemy', 'haram' (prohibited), etc. Symaira's case exemplifies this technique below as reported by her mother:

> [Symaira's maternal aunt stole one of her images from her mother's Instagram. She created a fictitious collage by juxtaposing her son's picture with Symaira's. She anonymously shared it online with an accompanied caption: '*we have sex and we love each other*.' The goal was to malign Symaira's reputation and suggest she was in an intimate relationship with the perpetrator's son.]

In other instances, images of modestly-dressed women were annotated with sentences such as, "I am a prostitute and can be reached at [home address] and [phone number]." In some cases, contact details of male family members were also shared, further amplifying the harm. In some instances, perpetrators falsely tried to tie victims to explicit material they had downloaded from adult websites (n=4). Hira's case illustrates this tactic below, as reported by her sister:

> [Her ex-boyfriend first sent her family a photograph of Hira (fully clothed), and in the next message, he sent an amateur porn video he got from the web where the faces of the people engaged in a sex act were blurred. Her parents were so horrified, they didn't even play the video to ascertain whether it was actually her or not.]

This class of NCIDA is effective despite being easily doctored content. IOs mentioned that this is partly due to limited levels of digital literacy, especially among the older generation, and partly due to the families' unfamiliarity with nude or sexual content – their emotional reactions are immediate and strong, so there is no psychological space for skepticism. Victims appear to intuit this, so instead of defending themselves to family members, they acquiesce to perpetrator demands.

4.2 Types of Perpetrators

The types of perpetrators we heard about goes beyond those of previous studies, who are predominantly former, current, or prospective sexual partners (see table 2). Among these are organized crime entities (24 out of 70) and adversaries (22) (see Figure 2). In the sections below, we present NCIDA cases involving non-intimate partners.

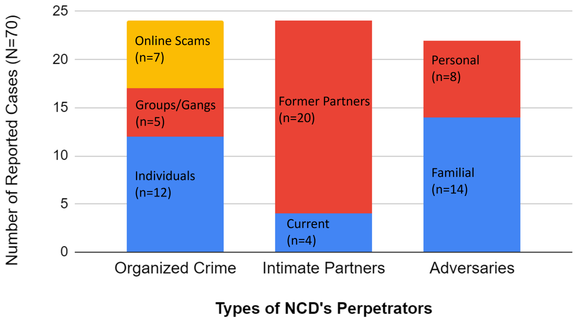

Figure 2: Perpetrators Categorization

4.2.1 Organized Crime. In our data, we found organized groups weaponizing NCIDA to extort and demand sexual favors. Out of the 24 instances, most (17) involved a physical component. Out of those half (12) were committed by individuals, while a few (5) involved an organized group comprising of both men and women. Additionally, a separate category involved online-only organized crime (7), with no offline communication with the victim. It was unclear whether these online-only perpetrators were operating as individuals or as part of a group.

Among individuals acting alone, we identified individuals posing as shopkeepers, salesmen, security guards, fake *imams* (religious leaders), house helpers, beauty parlor staff, and so on These perpetrators often had prior offline access to their victims, and began by establishing a degree of trust through business or religious interactions. As was true in Bushra's case, fake imams, exploited the victim's trust in religious figures, using fictitious pretenses to gain access to sensitive content that they later utilized for blackmail. The corresponding IO reported:

> [Bushra was facing marital difficulties. Someone tagged her to a fake imam's Facebook page who claimed to help with such marital issues. The fake imam instructed Bushra to share explicit photos and videos, committing to recite religious verses on these images [2] that he claimed would help her regain her husband's affection. Given her trust in religious figures, Bushra complied. During this time, her husband coincidentally called her to explore reconciliation efforts. This coincidence deepened her belief in the imam's healing powers, and Bushra thought Allah is doing all this for sure because of this imam's intervention. Subsequently, the imam increased the fee for his services, demanding gold as a form of payment for his services... When she was unable to fulfill his demands he threatened to expose the explicit content to her husband and her in-laws.]

In terms of organized groups, we found that they typically engage in complex, months-long schemes to ensnare victims. They work in teams, adopting false identities such as fictitious employers, real estate agents, or families interested in marriage. For instance, some pose as families seeking marriage for their children. According to IOs, their target is often families aspiring to secure their child's future by arranging a marriage with overseas Pakistanis (3 instances out of 70). Aleena's family fell victim to such a group that orchestrated a fake marriage, obtained explicit content after the 'marriage', and subsequently blackmailed the entire family for more dowry [49]. Aleena's family reported:

> [A neighbor informed Aleena's mother about a marriage proposal from a family visiting from abroad. Following mutual agreement, both families conducted the *nikah* [95], an Islamic marriage contract. Subsequently, the groom and his family departed, pledging to arrange Aleena's visa for her move. During this period, Aleena began exchanging messages with her 'husband' who was using a fake international phone number. Upon his request, she shared sensitive content, not assuming much given that he was now her spouse. However, as time passed, her family started receiving demands for more dowry in cash and gold from her in-laws, threatening to release the images otherwise.]

A variation of such a scheme initially entrapped men, but eventually targeted the women in the family, as is illustrated in Ali's case below. Note in these cases, even when a man is the target, women family members also suffer, as reported by Ali's mother:

> [The bride's family asked for a large sum of money (2 crore Rupees, US$70,000) as *Haq Mehar.* [2] Ali's family accepted the demand, and negotiated to paying a delayed Mehar only in the case of a divorce, a customary practice in Pakistan [48]. The bride lived with Ali's family for a short while, and during her stay, she secretly took private pictures of Ali's sisters and mother without their knowledge. Eventually, her family demanded a divorce coupled with the Mehar payment, threatening to disseminate explicit content of Ali's sisters.]

A third category of cases involved organized groups that only engaged with victims online, using platforms like social media or dating apps. Prior studies have explored such online scams perpetrated by 'transnational offenders' [61], emphasizing how these offenders (often masquerading as cis or transgender women primarily target men). While our findings mirror prior work that details male victims, we also found that women were also vulnerable to such crimes. In our data, we found men utilized elaborate and sophisticated schemes to gain access to women's explicit content, as is illustrated by Arooj's case:

> Arooj joined an anonymous live streaming platform... She was assigned a task to live stream *"down-blousing"* [52]. She did so in order to earn points (that can be converted into dollars). After a few days, she received a message from someone claiming to be from the platform, informing her that her down-blousing video had been uploaded on the platform. He offered to help her remove it, and instructed her to click a link he sent to her mobile phone. This led to her phone being hacked, sensitive content being stolen and subsequent extortion.

4.2.2 Personal Adversaries as NCIDA Perpetrators. In a number of cases (22 out of 70 cases), we found personal adversaries such as business competitors, classmates, work colleagues, extended family members, and in-laws used NCIDA to harm victims. These adversaries had a range of motives ranging from property disputes, to personal vendettas and jealousy. Revenge NCIDA was also a motive, where one party exposed the content of the other party, justifying their actions as: '*They revealed pictures of our sisters, so we are exposing their sisters' photos.*' In this category, perpetrators frequently lacked access to sensitive content, and resorted to fabricating content using the strategies outlined in Section 4.1.2. In Symaira's case where her aunt fabricated a collage (see Section 4.1.2), Symaira's mother alluded that the perpetrators' intent was a combination of revenge and coercion after their marriage proposal was rejected by the victim and her family. In another case, when Azoor's family accused her brother-in-law of her sister's murder, the accused and his family circulated real and doctored explicit content of Azoor and her late sister. This was an attempt to discredit the family's reputation and use NCIDA as leverage in the ongoing court case, eventually leading to Azoor's family dropping the charges under duress.

4.3 Threat Mechanisms and Their Effectiveness

Prior work on NCIDA has highlighted how viral public dissemination online is the goal or threat made by perpetrators [22, 44, 64, 76, 100, 101]. While our cases also included such threats, a more

[2] Haq Mehar, or Mehar, is a mandatory gift or token of respect given by the husband to the wife as part of an Islamic marriage contract [67].

common threat was to disclose sensitive content to family members of the victim, especially male family members. To our knowledge, such threats have not been reported in Western contexts (see 2). We found that in cases in which public disclosure had not yet occurred (51 out of 70), the perpetrators appeared to have a notion of escalating disclosures, starting with the victim, to a woman family member, to male family members, and finally the public at large. We elaborate on each of these steps below:

4.3.1 Step 1: Gathering Family Contact Information. Perpetrators use a variety of methods to collect contact details of victims' family members, through, e.g., unauthorized access to victims' call detail records (CDRs) (6 out of 70) and exploiting social media features (4). In Ayesha's case (Section 4.1.2), the offender acquired her CDRs to access her husband and family's contact details. An IO claimed that some telecom employees sell victims' call records to perpetrators for 4,000-5,000 rupees (US$12-15).

4.3.2 Step 2: Contacting Victims. We found that once perpetrators had acquired family contact details, they used overt as well as covert tactics to escalate threats and intimidate victims (31 out of 70 cases). Overt actions included sending fictitious package tracking details to the victim, claiming that sensitive material was mailed to the victim's family. In Arooj's case, her classmate fabricated her WhatsApp profile picture into explicit content to coerce sexual favors. When she resisted, he claimed to have sent the material to her brother. The victim reported:

> [He sent me a picture of a parcel this morning and texted that he had mailed sensitive pictures of me to my brother.]

Covert intimidation strategies involved technical exploits such as using untraceable numbers generated via VPN, using 'one-time view' and 'delete for all' features to remove traces of direct threats, as well as using anonymous social media accounts to share compromising content. One of the victims who participated in a follow-up interview reported:

> *"He sent me a few screenshots through WhatsApp of a fake profile he had created on Facebook, and before I could comprehend what was happening, everything disappeared as it was a 'one-time view' only."*

4.3.3 Step 3: Contacting Victim's Women Family Members. In cases where family disclosures (partial or full) occurred (39 out of 70 cases), half (20) of the perpetrators first disclosed to women family members of the victim – mothers, sisters, or sister-in-laws. IOs highlighted that this approach hinges on the assumption that women family members are more susceptible to coercion, given the societal patriarchal norms around honor. Perpetrators capitalize on this vulnerability, approaching women family members to pressure the primary victim. One IO explained:

> *"[Perpetrators] are well aware that all the mother will do is slap [the victim] twice, and then they themselves will become afraid of what is going to happen."*

In Maryam's case, her husband contacted her mother and threatened to disclose sensitive content to her father in the hopes that her mother would persuade Maryam to stay in a secretive, but abusive marriage. The corresponding IO reported:

> [The perpetrator escalated by involving her mother. He threatened to expose their sexually explicit content to her father. This manipulation coerced Maryam's mother to persuade her to reconsider staying in the marriage fearing severe consequences if her father discovered the content.]

4.3.4 Step 4: Contacting Male Family Members and Subsequent Public Disclosure. The next step in NCIDA-related threats involves exposing sensitive information to male family members, typically coupled with threats to publicly broadcast the content or sharing it widely within the victims' family/social circle (19 cases). Many Pakistani families prize reputational "honor," and families fear damage to it. We found that perpetrators employed tactics like leveraging trending hashtags for rapid virality (5 cases), posting content through anonymous accounts (15), and approaching male family members in the company of their acquaintances (6) to intensify humiliation. Faiza's ordeal with her ex-boyfriend exemplifies this tactic, which an IO reported:

> [In retaliation, he sent explicit content to her mother. When this level of escalation failed to have the desired impact, he escalated by sending semi-explicit content to her brother and father, and demanded a meeting. When the meeting took place, the perpetrator showed Faiza's explicit content to the father in front of his friends on a big screen, pressuring him to break the engagement.]

4.3.5 Effectiveness of Threats. Prior research suggests that NCIDA victims often respond to threats in one of two ways. Those in ongoing intimate relationships typically succumb to the perpetrators goals of control. Those outside of intimate relationships ignore the NCIDA, use in-app reporting tools, or seek aid from law enforcement [20, 99, 104]. The latter class of victims, in other words, do not cower in the face of the threat. Our victim participants in Pakistan, however, frequently complied with perpetrators even when there was no intimate relationship, out of *extreme fear* of potential repercussions. Victims are thus easily entrapped in a cycle of extortion. In one case, extortion lasted for 1.5 years, ending only when the victim became bankrupt.

Perpetrators often employ relentless pressure tactics on victims. For instance, a perpetrator sent countdown messages to a victim until he would send the images to her father lest she meets his monetary demands: (*"message 1: 20 mins, message 2: 19 mins, message 3: 18 mins,..."*). An IO reported:

> *"[Perpetrators] often initiate blackmail during the night or on weekends, deliberately creating a sense of urgency that leaves victims with limited options and support. This urgency is exacerbated by the fact that most helplines, including ours, are not as active during weekends. Perpetrators often repeatedly claim 'I am about to send it, I am about to send it' to intensify this urgency."*

4.4 Limited Support and Consequences Beyond the Crime

Our findings on individual consequences faced by victims of NCIDA echo prior research, including psychological, reputational, financial, social, and physical harms. However, our findings deviated when it came to anticipated social support for victims. While prior literature often portrays families and social circles as sources of support [73, 91], our findings reveal an absence of substantial support networks. Instead, we found victims encountered negative repercussions from within their families and extended social circles. This section details the limited support mechanisms and the hardships faced by victims and their families due to the absence of adequate support.

4.4.1 Limited Familial Support. In contrast to prior studies from within South Asia [57, 74], we found that victims receive limited support from family members, peers, and law enforcement. There is a lot of victim-blaming. In most of the cases (56 out of 70), victims felt guilt for their perceived moral failings (*"My parents think I am a good daughter but I am not"*) or for damaging family reputation. Many victims began their statements with statements such as *"I have ruined my family's reputation..."*). In cases where the victims engaged in premarital or extramarital sexual relationships and/or sharing explicit content with men they were not married to, the victims often felt great guilt: (*"I've made a big mistake, and now only Allah can offer forgiveness..."*). This self-blame intensifies when the explicit content involves secret actual who are now using this content to blackmail.

We observed that victims often expressed apprehension about receiving support from their families, especially in cases involving the disclosure of sexually explicit content. When they approached LEAs, they frequently expressed a desire to keep their families uninvolved (*"If my family has to be brought into this, I'd rather not proceed. I want to prevent their involvement in any way."*).

Meanwhile, our observations revealed that in some cases, families offered conditional support that was contingent on factors such as the nature of the content. Non-consensual or coerced material typically received more substantial family support compared to consensual and explicit content, especially when the coercion was evident within the content. Additionally, family support tends to be stronger in cases where the relationship between the victim and perpetrator is formally recognized and approved, such as in the case of arranged marriages. Moreover, family perception of the victim's maturity level is influential; younger or less experienced victims usually receive more familial backing compared to working and independent women, particularly from middle to lower-middle-class backgrounds.

This difference in the nature of support significantly influences the experience and outcomes for victims. The threat mechanism involving disclosure to family members highlights the role family members play in further aggravating the impact of such abuse. As an NGO worker highlighted in a previous South Asian study: *"...If the patriarchal society does not react, then a blackmailer has no power" [74].* This statement emphasizes the critical role family can play in reducing the efficacy of threats posed by perpetrators.

4.4.2 Severity of Consequences. In prior work, victims primarily suffer as individuals, experiencing financial setbacks and reputational damage. While such harms are terrible, they pale in comparison to what Pakistani victims and their families suffer. We found that the consequences of NCIDA in Pakistan differ in two main ways: intensity, and number of people who suffer.

Heightened Severity for the Primary Victim: In Pakistan, the repercussions of NCIDA for the primary victim are notably amplified. Not only are they targeted by perpetrators, but societal and familial backlash is also common. In our study, for instance, about half of the victims reported experiencing familial rebuke (34 out of 70, including 32 men and 2 men) and violence (20, all women) following disclosure to family, while others expressed fear of both consequences. Some endured physical confinement (5, all women) or even death, reportedly through murder by family members (3, all women) as reported by participants and IOs. We have included some illustrative cases that demonstrate the gravity of the consequences that victims face as a result of NCIDA.

- **Sara's tragedy (Reported by an IO):** [Sara, who comes from a deeply religious family that places a high value on honor, wanted to leave her abusive relationship, but her ex-boyfriend threatened to expose explicit content to her brother. She sought help at CCW, asking not to inform her brother given his history with outbursts of anger. Her ex-boyfriend later sent the content to him, leading to a confrontation where her brother expressed a desire to harm them both. The IO reported that: *"[The victim's brother] said she let our honor down, and I cannot rest knowing that she has brought this upon us. She could have told us earlier. I'll kill both of them before this becomes public."* Tragically, Sara sent a distressing message hinting at suicide, and shortly afterwards, she passed away, with her brother claiming it was due to a sudden cardiac arrest.]
- **Zarish's ordeal (reported by an IO):** [After a significant delay, Zarish returned for a follow-up to the LEA. She described being placed under house arrest by her family due to disclosure of her explicit content by her ex-boyfriend. Her family was eager to marry her off to prevent any harm to family's reputation and the potential risk to her sisters' marital prospects. She told that she was isolated at home, with no one speaking to her. Her mother even physically abused me on several occasions. Her brother and father were fervently searching for a suitor, eager to marry her off and distance themselves from the situation.]
- **A Father's Outrage (Reported by the victim's father):** [A father accompanied his daughter to file a complaint against his daughter's friend with whom she had a sexual relationship and intimate content was disclosed. Clear marks of physical abuse marred her face. When the authorities inquired about the injuries, he confessed that he is responsible for those marks. He struck her out of disbelief that she could jeopardize his family's reputation — a reputation he has spent his entire life building.]

Beyond severe physical harm, NCIDA often result in strained relationships, as exemplified in Ayesha's case (Section 4.1.2), compromised marital prospects as seen in Symaira's situation (Section 4.1.2), and forced marriages similar to Zarish's experience discussed above.

Collective Impact on Families: While in prior work NCIDA repercussions tend to be limited to the victim, our data shows that in Pakistan the ramifications affect the broader family, particularly resulting in collective reputational and financial harm. For instance, Ali's mother (Section 4.2.1) reported her concern about the stigma that comes from being associated with prostitution:

> *"Imagine the anguish of confronting my brother-in-law or facing my family if these pictures and videos went viral, painting us as prostitutes. My husband was a respected man, and to face such scandal, especially after his passing, is unbearable. People are bound to believe the rumors, thinking that I've been waiting for his death to indulge in such actions."*

Financial repercussions are also not borne by the victim alone. The whole family shoulders the burden, be it through paying ransom, as with Aleena and Ali (Section 4.2.1), or the victim depleting family savings, as seen in Ayesha's case in Section 4.1.2. Moreover, Bismah, a victim, reported:

> [Ever since my father's death, I am the sole provider for my family. My ex-boyfriend exposed compromising content to my employers, leading to repeated job losses. Having changed jobs four times and missed three months' wages, my family's financial reserves have depleted. This ordeal has deeply impacted both me and my family.]

4.5 Preferred Remedies

Previous studies suggest that reparations for NCIDA have shifted from a punitive model to a restorative justice approach aimed at providing support to victims and promoting social goods [39, 78]. We found that the punitive model was primary among our participants, and that they also sought restorative justice. Thus, our participants first sought punitive actions like content removal from the perpetrator's devices, legal summons, arrest, corporal punishment, or, in some cases, a court trial. On top of those consequences, our participants were also concerned with safeguarding and upholding their family's reputation. They thus expressed interest in restorative remedies such as a written guarantee of NCIDA cessation; a private legal apology — a signed statement carrying legal consequences; and/or a public apology coupled with an admission of fabricating content. Content removal from public platforms and private devices was a consistent desire across all victims (70 out of 70); victims also sought out-of-court settlements and monetary compensation.

Our study identified a pattern in which the remedy sought was related to the stage of disclosure. When no disclosure occurred (31 out of 70 cases), women victims of NCIDA, particularly those involving sexually explicit content (17), preferred content removal alongside a signed written guarantee of NCIDA cessation and a private legal apology. These victims did not want strict punitive actions against perpetrators, and IOs explained that this was largely because they did not want their identity disclosed in a legal case. Seeking punitive justice can also be traumatizing for victims, with the possibility of uncomfortable interactions with male police officers, retaliation from perpetrators, and retraumatization during trial. An IO reported how this process plays out:

> *"This guarantee coupled with a private apology takes the form of a government document, an affidavit. The affidavit is legally binding, and affirms that the perpetrator will abstain from similar actions in the future. The corresponding IO acts as a witness, possessing the authority to arrest the perpetrator if they breach the agreement.*

When selective disclosures have already been made to family members, victims seek different remedies depending on the family member concerned. In the case of disclosure to women family members, the preferred remedies involved a combination of content removal with a physical remand that is often accompanied with mild corporal punishment. According to IOs, women family members, especially mothers, express a desire for punitive measures against the perpetrators to ensure the perpetrator bends to the demands of a written guarantee. However, going beyond minor punitive actions was not preferred, given the likelihood of disclosure to male family members or the public at large during legal proceedings.

In contrast, when selective disclosures occurred among male family members, the preferred remedies were more stringent, including filing a First Information Report (FIR) – a legal document that sets the process of criminal justice in motion [5], initiating court proceedings, and finally settling out-of-court while obtaining a written apology and NCIDA cessation guarantee.

Upon public content disclosure, victims and families transitioned from seeking private to demanding public apologies. This shift results from the profound impact of public exposure on reputation and family honor, necessitating not just content removal and legal action but also a public apology that explicitly acknowledges wrongdoing, states motives and content creation strategies, and highlights that the content was fabricated. This was true in Symaira's case (from Section 4.1.2), when her family reported:

> [Symaira's family insisted that the perpetrators upload an apology video on the same social media platform and explain the creation and uploading of the collage, clarify their intentions, and in that video apology, affirm Symaira's innocence.]

5 DISCUSSION

Our findings underscore the significant differences between NCIDA in Pakistan and in the West. These differences are underscored even by the fact that the previous literature discusses NCIDA as NCII [1, 33, 34, 98]: "non-consensual intimate image," as if intimate imagery were required for these abuses. Our findings provoke an expansion of the underlying concept, and also enable the sketching of a broadly applicable theory of NCIDA. We discuss both below.

5.1 Key NCIDA Differences: Pakistan and the West

Overall, we find in Pakistan that a much broader class of content can become an NCIDA, and that the consequences for NCIDA are much more severe than has been previously reported [11, 14, 16, 22, 23, 33, 35, 61, 64, 71, 86, 104]. See Table 5 for a summary of these differences. Many, if not all, of the differences can be traced to the underlying culture of Pakistan, where a strong patriarchy often subscribes to traditional notions of honor, and in which a woman's chastity and modesty are significant concerns of male family members [27]. As a result, content – such as a selfie in a sleeveless blouse – that, say, North Americans would readily post publicly themselves, can be profoundly sensitive in Pakistan; and threats of NCIDA – often based on content in which the victim played no problematic role *even by the standards of the surrounding society* – appear to lead to a spiral of extortion. And, because it is so easy to generate potential NCIDA content, there seem to be additional classes of perpetrators who have no prior romantic or sexual relationship with their victims. Organized criminal groups and acquaintances holding a grudge use the easy on-ramp of NCIDA to intimidate and extort victims, without pre-existing romantic or sexual context. That is in stark contrast with what is reported in Western NCIDA cases, which almost always involve former, current, or prospective intimate partners, or people with voyeuristic intent [61].

The extent to which NCIDA and its consequences differ between Pakistan and the West suggest an overhaul of the way that NCIDA is described and contextualized, so as to ensure a more comprehensive view that is not limited to Western contexts. First of all, it should be highlighted that NCIDA is very much in the eye of the beholding society. Previous literature, with the exception of Sambasivan et al. [73], has not acknowledged this point, probably because work so far has predominantly assumed a Western environment, as we showed in Tables 1 and 2. What counts as an NCIDA, therefore, should be broadened, and the cultural context of NCIDA ought to be taken far more seriously. We also recommend as future work, explorations of NCIDA in non-Western countries beyond South Asia, as some would likely exhibit elements not seen before or in this paper.

5.2 A Preliminary Theory of NCIDA

When combined with what is known from the previous literature, our findings suggest a deeper theory of NCIDA, a preliminary version of which we outline here: Drawing from the above discussion, the core of the theory is that NCIDA exist in relation to what the local culture finds socially and morally acceptable, especially with regards to romance, sexuality, marriage, and public visibility. NCIDA work in part because both perpetrators and victims have similar notions of what is *not* appropriate for public consumption. Perpetrators use this knowledge to cause harm or make threats; and, victims are hurt or fear harm, because they subscribe to the same definition of propriety. Thus for example, little short of nude imagery tends to become an NCIDA in the United States; whereas a clothed couple holding hands can be NCIDA fodder in Pakistan.

Another element of the theory is that the radius and severity of NCIDA's impact correlates with the strength of the corresponding norms. In Pakistan, where patriarchal expectations can be both restrictive and potent, NCIDA impacts more people (i.e., the immediate victim *and* family members), result in more severe consequences (e.g., suicides and honor killings), and trigger greater fear more easily (e.g., extortion based on juxtaposed imagery without any "real" compromising content). A contrasting case is offered by previous research in the United States, in which reports do not mention family members being implicated (though they often feel vicarious pain from empathizing with victims) [66], and deaths arising from NCIDA appear much less common [53].

The theory may seem straightforward, even obvious in retrospect, but it has not been asserted previously in this form [34]. And, making the theory explicit permits some degree of prediction. For example, we predict that cultures that are relatively more open with nudity see a narrower set of NCIDA content than those that hold all nudity to be private, and that the consequences of disclosures are less severe on average. Future work could seek to confirm whether this is the case in countries such as those in Northern Europe.

If the theory bears out, it could be useful, say, to social media companies in their efforts to address NCIDA. It might be possible, for example, to create classifications of countries based on their prevailing norms, and to anticipate NCIDA to some degree, though that would not eliminate the need for country-specific attention and adaptation, as we discuss next.

5.3 Recommendations

Before discussing novel recommendations, we emphasize that most of the recommendations made in the existing literature also apply to the Pakistani context. To begin, technology development should itself involve victim perspectives [8].There should be accessible in-app reporting features to enable swift response to threats or actual disclosures [62]. Deindexation services to help limit dissemination of sensitive content should be expanded [21]. Tools designed for reporting evidence of online misconduct should be made broadly available [26, 91]. Of course, such tools need to be localized for language and social context.

We also strongly reinforce existing calls to treat NCIDA as criminal activity [11, 14, 22, 23, 33, 35, 36, 65, 71, 104]. Pakistani examples re-emphasize the traumatic impact they can have on victims and their families, as well as the malicious intent by which they are perpetrated. We agree with arguments that consider NCIDA a form of violence [33, 71], and they should not be granted free-speech protections, any more than incitements to physical violence should be. Furthermore, based on remedies sought by our participants, we advocate against a one-size-fits-all solution [78, 80, 81], and propose the integration of restorative justice strategies alongside punitive measures in the design process.

In addition, our findings also suggest recommendations not previously made in the literature, both for the Pakistani context specifically and for globally minded entities – researchers, social media companies, and governments.

5.3.1 *Recommendations for Pakistan.*

Through a secular liberal lens, it is difficult not to criticize the victim-blaming that appears to happen in some Pakistani families, even when the victims are wholly innocent of offenses defined by the prevailing patriarchy. But changing that culture seems out of reach without larger shifts in Pakistani society, and in any case is out of this paper's scope. Therefore, following Sultana et al. [92], who urge more modest forms of action, we believe a number of efforts could help prevent or mitigate the impact of NCIDA in Pakistan, even with cultural norms remaining largely as they are.

One clear need is greater digital media literacy in the general public, both with respect to the dangers of NCIDA as well as the fact that critical inspection of seemingly sensitive images is required. Public service message campaigns conducted through broadcast news media and/or social media ads could serve to raise general awareness, with the goal of preventing NCIDA victimization and inviting critical reflection in cases of manufactured NCIDA content. The impact of such campaigns varies, but Pakistan has seen

Dimension	Findings from Previous Work	New Findings from This Paper
Perpetrators	Current, former, and prospective intimate partners	Organized crime groups
	Transnational offenders targeting men	Personal adversaries with not sexual/romantic intent (e.g., classmates, colleagues, relatives)
	Voyeuristic strangers	
	Acquaintances including friends, family members and relatives	
Content	Sexually explicit (real) imagery	Non-sexual imagery of friendly interactions between unmarried couples
	Sexually explicit deepfake imagery	Imagery juxtaposing victims (in publicly acceptable poses) with sexually explicit others
		Imagery of victims (in publicly acceptable poses) annotated with defamatory text of a sexual nature
Threat Mechanism	Disclosure to victim's social circle	Disclosure to male family members
	Disclosure to general public	4-stage threat escalation (see Section 4.3)
Consequences	Individual level: Emotional distress, Physical self-harm (including suicide), Social consequences, Financial/livelihood consequences	Individual level: Murder (honor killing), Domestic abuse and control, Forced marriage
		Family level: Reputational damage, Social isolation, Financial/livelihood consequences
Preferred Remedies	Justice: Public shaming, Criminal penalties, Financial compensation, Restorative justice (incl. private apologies)	Justice: Public apology (only if disclosure went public), Public admission of fabricated content (only if content was fabricated and disclosure went public), Private legal apology (signed statement carrying legal consequences), Guarantees of NCD cessation
	Content removal from public sites	Content removal from private storage (in addition to public sites)

Table 5: Summary of findings from previous literature and new findings mentioned in this paper. The rightmost column represents aspects of NCIDA that we encountered in Pakistan that have not been mentioned in the research literature thus far.

success with recent campaigns such as the Sukh Initiative for family planning [56], and more recently, messaging around COVID protocols [69].

In terms of technical and design recommendations, we recommend that apps that allow video calls (WhatsApp, FaceTime, etc.) should allow users to forbid others from taking a screenshot during an active video call, as is the case for many Muslim dating apps [55, 72]. In some countries, this option should be enabled by default, with an opt-out option. Second, social media platforms should adopt a feature akin to de-indexing in search engines [21]. When users report a post as an NCD, the reported content's visibility should be limited (shadow banned [75]) *to the reporting user's connections* until reviewed by a human moderator. The moderators should also be chosen for their understanding of local societal norms. Third, messaging apps like WhatsApp should enable users to flag threatening or otherwise abusive evaporating 'one-time view' messages. If violations are found, social media companies should generate reports for law enforcement or provide access to stored content under specific conditions. Content not reported to law enforcement should be deleted after a designated period, e.g., two years.

5.3.2 *Global Recommendations.*

As noted in the Discussion, a key conclusion of our work is that NCIDA vary by cultural context. Thus, responses to them must be tailored, probably at the country level, but possibly in more fine-grained fashion. (Some countries, for example, have parallel laws that apply to different religious groups [90], and policies for NCIDA may require a similar structure.) Researchers, content platforms, and others working with NCIDA across countries should be vigilant to differences by culture, and to draw conclusions or make recommendations accordingly.

At the same time, there are recommendations applicable at a global level, for social media companies and national governments. Above all, one overarching recommendation is to hold social media companies more responsible for the problems caused by NCIDA. The existing literature on NCIDA in the West does not mention the additional stress placed on law enforcement agencies – presumably, there is some, but the impact may be minor. As we saw indirectly through our findings, however, Pakistani law enforcement expends considerable resources to address the fall-out of NCIDA. Several of our officer participants pointed this out explicitly, and one put it succinctly: *"Technically these social media companies should pay for [raids on NCIDA perpetrators] as we are brushing dust created by these platforms."*

Social media firms are already under some pressure to address NCIDA [77], but we further suggest that they should bear some of the societal cost of NCIDA. NCIDA, after all, is effectively a new class of problem created by tech companies. Drawing inspiration from "oil spill liability funds" [96] – in which oil companies pay into a fund that is used in the event of an oil spill – we suggest that tech companies form an NCIDA liability fund in countries in which they operate, to help mitigate the effects of NCIDA. Funds could be used to support relevant law enforcement divisions, pay for research on local NCIDA, offer support to victims in various forms, and increase awareness among potential victims.

Next, what NCIDA victims – both from the existing literature and in our study – wish for most is for problematic content to be deleted *everywhere*. Social media companies should therefore develop robust semi-automated systems for swift detection and removal of NCIDA content, based on contextual, localized guidelines. This activity should be contextualized, proactive, and follow feminist guidelines of consent [38].

Third, social media companies should coordinate more closely with local law enforcement agencies (LEAs). From our findings, it became evident that there is a difference in the interpretation of what constitutes NCIDA between Pakistan and the West. This difference could pose a challenge for IOs in obtaining the necessary data to catch the culprits which can significantly increase the workload of IOs and elevate the risk for the victims. Future research should investigate the potential nature of collaboration between platforms and LEAs and how it can be enforced given the limited influence LMIC countries like Pakistan can exert over large tech companies.

Fourth, social media platforms should form a consortium dedicated to addressing NCIDA. As we saw in our findings, one challenge for victims is the fact that content can live across platforms, making it insufficient to remove content from just one. Through consortium dedicated to NCIDA, platforms could collaborate to ensure that NCIDA content deleted from one platform is deleted on others too.

Finally, we recommend that each national government mandate recommendations it deems worthwhile through policy. Social media firms draw considerable revenue from their operations in any given country, yet often, they manage to avoid local taxes [82]. For example, in Pakistan, none of ByteDance (parent company of TikTok), Google, or Meta pay taxes [32]. Thus, governments should not hesitate to demand that social media companies comply with regulations that serve their citizens, or pay their share to minimize the impact of NCIDA, for the privilege of operating in their countries.

6 LIMITATIONS

Our study has methodological and sampling limitations. It primarily includes victims who sought assistance from relevant organizations, likely a group with a greater tolerance for NCIDA, as in all cases, discussion with the IOs required going into the detail of their cases. While our sample included only women and men victims, we are aware that NCIDA affect marginalized individuals of all genders, particularly non-cisgender or non-binary individuals, who may encounter additional stigma and challenges in coming forward. Additionally, while acknowledging the significance of including perpetrators' perspectives in the study, our study focused solely on the viewpoints of victims and investigation officers from LEAs. Future research could delve into highlighting the perpetrators' perspectives within the domain of NCIDA, IBSA, and TFSA.

7 CONCLUSION

This paper expands the exploration of NCIDA beyond Western, Educated, Industrialized, Rich, and Democratic (WEIRD) contexts, delving into diverse cultural landscapes. Our study within a deeply rooted honor-based patriarchal context highlights the broader interpretation of inappropriate behavior compared to Western norms. With such fragile sensitivity of content in this context, NCIDA predominantly target women, leveraging the disclosure to male family members as a primary threat. Cultural values like honor, patriarchy, and religion amplify the range and consequences of NCIDA, extending their association with violence beyond Intimate Partner Violence (IPV) to include honor-based abuse. These factors increase the accessibility of offenses, attracting a wider range of perpetrators. We propose actionable recommendations for stakeholders, emphasizing the need for culturally-aware design and platform policies. This research contributes to a more comprehensive understanding of NCIDA, with potential implications for similar investigations worldwide.

ACKNOWLEDGMENTS

We would like to sincerely thank all our study participants and our collaborators at the cybercrime wing of the federal agency and the NGO for their immense support in conducting this research. We are also grateful to our CHI Associate Chairs and reviewers for their thoughtful comments, which have significantly contributed to the improvement of this paper.

REFERENCES

[1] 2015. Stop Non-Consensual Intimate Image Abuse. https://stopncii.org/

[2] Oren Asman. 2008. Qur'anic healing for spiritual ailments: between tradition, religious law and contemporary law. *Med. & L.* 27 (2008), 259.

[3] Yara Barrense-Dias, André Berchtold, Joan-Carles Surís, and Christina Akre. 2017. Sexting and the definition issue. *Journal of adolescent health* 61, 5 (2017), 544–554.

[4] Samantha Bates. 2017. Revenge porn and mental health: A qualitative analysis of the mental health effects of revenge porn on female survivors. *Feminist Criminology* 12, 1 (2017), 22–42.

[5] Zulekha Begum. 2023. Analysis of FIR with Case Judgment. *Issue 2 Indian JL & Legal Rsch.* 5 (2023), 1.

[6] Rosanna Bellini, Kevin Lee, Megan A. Brown, Jeremy Shaffer, Rasika Bhalerao, and Thomas Ristenpart. 2023. The Digital-Safety Risks of Financial Technologies for Survivors of Intimate Partner Violence. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 87–104. https://www.usenix.org/conference/usenixsecurity23/presentation/bellini

[7] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L Mazurek, Dana Cuomo, et al. 2023. SoK: Safer Digital-Safety Research Involving At-Risk Users. *arXiv preprint arXiv:2309.00735* (2023).

[8] Lindsay Blackwell, Jill Dimond, Sarita Schoenebeck, and Cliff Lampe. 2017. Classification and its consequences for online harassment: Design insights from heartmob. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–19.

[9] Richard E Boyatzis. 1998. *Transforming qualitative information: Thematic analysis and code development.* sage.

[10] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[11] Danielle Keats Citron and Mary Anne Franks. 2014. Criminalizing revenge porn. *Wake Forest L. Rev.* 49 (2014), 345.

[12] Shamita Das Dasgupta. 2000. Charting the course: An overview of domestic violence in the South Asian community in the United States. *Journal of social distress and the homeless* 9, 3 (2000), 173–185.

[13] Dawn. 2022. Women Committed Suicide. (2022). https://www.dawn.com/news/1713205

[14] Jill P Dimond, Casey Fiesler, and Amy S Bruckman. 2011. Domestic violence and information communication technologies. *Interacting with computers* 23, 5 (2011), 413–421.

[15] Nicola Döring. 2014. Consensual sexting among adolescents: Risk prevention through abstinence education or safer sexting. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 8, 1 (2014), 9.

[16] Asia A Eaton, Sofia Noori, Amy Bonomi, Dionne P Stephens, and Tameka L Gillum. 2021. Nonconsensual porn as a form of intimate partner violence: Using the power and control wheel to understand nonconsensual porn perpetration in intimate relationships. *Trauma, violence, & abuse* 22, 5 (2021), 1140–1154.

[17] Elizabeth Englander. 2015. Coerced sexting and revenge porn among teens. *Bullying, teen aggression & social media* 1, 2 (2015), 19–21.

[18] Elizabeth Kandel Englander and Meghan McCoy. 2017. Pressured sexting and revenge porn in a sample of Massachusetts adolescents. *International Journal of Technoethics (IJT)* 8, 2 (2017), 16–25.

[19] Christopher J Ferguson. 2011. Sexting behaviors among young Hispanic women: Incidence and association with other high-risk sexual behaviors. *Psychiatric quarterly* 82 (2011), 239–243.

[20] 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.

[21] Leandro Ayres França and Jéssica Veleda Quevedo. 2020. Project Leaked: 1 Research on Non-Consensual sharing of Intimate Images in Brazil 2. *International journal of cyber criminology* 14, 1 (2020), 1–28.

[22] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise" How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–13.

[23] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM on human-computer interaction* 1, CSCW (2017), 1–22.

[24] Aina M Gassó, Katrin Mueller-Johnson, and Esperanza L Gómez-Durán. 2021. Victimization as a result of non-consensual dissemination of sexting and psychopathology correlates: An exploratory analysis. *International journal of environmental research and public health* 18, 12 (2021), 6564.

[25] Kareem Gibson. 2020. Deepfakes and involuntary pornography: can our current legal framework address this technology? *Wayne L. Rev.* 66 (2020), 259.

[26] Nitesh Goyal, Leslie Park, and Lucy Vasserman. 2022. " You have to prove the threat is real": Understanding the needs of Female Journalists and Activists to Document and Report Online Harassment. In *CHI Conference on Human Factors in Computing Systems*. 1–17.

[27] Manisha Gupte. 2015. The role of 'honor'in violence against South Asian women in the United States. *Manavi Occasional Paper* 11 (2015).

[28] Abdul Hadi. 2017. Patriarchy and gender-based violence in Pakistan. *European Journal of Social Science Education and Research* 4, 4 (2017), 289–296.

[29] 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.

[30] Bridget A Harris and Delanie Woodlock. 2019. Digital coercive control: Insights from two landmark domestic violence studies. *The British Journal of Criminology* 59, 3 (2019), 530–550.

[31] Douglas Harris. 2018. Deepfakes: False pornography is here and the law cannot protect you. *Duke L. & Tech. Rev.* 17 (2018), 99.

[32] Taimoor Hassan. 2023. Does big tech evade taxes in Pakistan and what can we do about it? https://profit.pakistantoday.com.pk/2023/08/07/does-big-tech-evade-taxes-in-pakistan-and-what-can-we-do-about-it/#:~:text=As%20a%20branch%20liaison%20office,registration%2C%20according%20to%20the%20study.

[33] Nicola Henry, Asher Flynn, and Anastasia Powell. 2019. Image-based sexual abuse: Victims and perpetrators. *Trends and Issues in Crime and Criminal Justice* 572 (2019), 1–19.

[34] Nicola Henry, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell, and Adrian J Scott. 2020. *Image-based sexual abuse: A study on the causes and consequences of non-consensual nude or sexual imagery.* Routledge.

[35] Nicola Henry and Anastasia Powell. 2016. Sexual violence in the digital age: The scope and limits of criminal law. *Social & legal studies* 25, 4 (2016), 397–418.

[36] Nicola Henry, Anastasia Powell, and Asher Flynn. 2017. Not just 'revenge pornography': Australians' experiences of image-based abuse. *A summary report. Melbourne: RMIT University* (2017).

[37] Qian Hongdao, Muhammad Bilawal Khaskheli, Hafiz Abdul Rehman Saleem, Jonathan Gsell Mapa, and Sughra Bibi. 2018. Honor killing phenomena in Pakistan. *JL Pol'y & Globalization* 73 (2018), 169.

[38] Jane Im, Jill Dimond, Melody Berton, Una Lee, Katherine Mustelier, Mark S Ackerman, and Eric Gilbert. 2021. Yes: Affirmative consent as a theoretical framework for understanding and imagining social platforms. In *Proceedings of the 2021 CHI conference on human factors in computing systems*. 1–18.

[39] Jane Im, Sarita Schoenebeck, Marilyn Iriarte, Gabriel Grill, Daricia Wilkinson, Amna Batool, Rahaf Alharbi, Audrey Funwie, Tergel Gankhuu, Eric Gilbert, et al. 2022. Women's Perspectives on Harm and Justice after Online Harassment. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–23.

[40] Michelle A Krieger. 2017. Unpacking "sexting": A systematic review of nonconsensual sexting in legal, educational, and psychological literatures. *Trauma, Violence, & Abuse* 18, 5 (2017), 593–601.

[41] Ada Lerner, Helen Yuxun He, Anna Kawakami, Silvia Catherine Zeamer, and Roberto Hoyle. 2020. Privacy and activism in the transgender community. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–13.

[42] Ruth Lewis and Sundari Anitha. 2023. Upskirting: A systematic literature review. *Trauma, Violence, & Abuse* 24, 3 (2023), 2003–2018.

[43] Charles Lindholm. 1982. *Generosity and jealousy: the Swat Pukhtun of northern Pakistan.* Columbia University Press.

[44] Jacqueline D Lipton. 2014. Repairing Online Reputation: A New Multi-Modal Regulatory Approach. (2014).

[45] Amy Lyndon, Jennifer Bonds-Raacke, and Alyssa D Cratty. 2011. College students' Facebook stalking of ex-partners. *Cyberpsychology, Behavior, and Social Networking* 14, 12 (2011), 711–716.

[46] Sophie Maddocks. 2018. From non-consensual pornography to image-based sexual abuse: Charting the course of a problem with many names. *Australian Feminist Studies* 33, 97 (2018), 345–361.

[47] Sophie Maddocks. 2022. Feminism, activism and non-consensual pornography: Analyzing efforts to end "revenge porn" in the United States. *Feminist Media Studies* 22, 7 (2022), 1641–1656.

[48] Attia Madni and Rabia Zulfiqar. 2022. Khula under Islamic Law & Judicial Practice in Pakistan: A No Fault Divorce Regime. *Journal of Educational Management and Social Sciences* 3, 1 (2022), 38–46.

[49] Momoe Makino. 2019. Marriage, dowry, and women's status in rural Punjab, Pakistan. *Journal of population economics* 32, 3 (2019), 769–797.

[50] Alison Marganski and Lisa Melander. 2018. Intimate partner violence victimization in the cyber and real world: Examining the extent of cyber aggression experiences and its association with in-person dating violence. *Journal of interpersonal violence* 33, 7 (2018), 1071–1095.

[51] Alice E Marwick. 2017. Scandal or sex crime? Gendered privacy and the celebrity nude photo leaks. *Ethics and Information Technology* 19 (2017), 177–191.

[52] Clare McGlynn and Julia Downes. 2015. Why we need a new law to combat'upskirting'and'downblousing'. (2015).

[53] Clare McGlynn and Erika Rackley. 2017. Image-based sexual abuse. *Oxford Journal of Legal Studies* 37, 3 (2017), 534–561.

[54] Tahlee Mckinlay and Tiffany Lavis. 2020. Why did she send it in the first place? Victim blame in the context of 'revenge porn'. *Psychiatry, psychology and law* 27, 3 (2020), 386–396.

[55] Muzz. 2023. Muzz is having a glow up. https://muzz.com/bn-BD/blog/muzz/disappearing-messages-replying-deleting-texts

[56] H Najmi, H Ahmed, GM Halepota, R Fatima, A Yaqoob, A Latif, W Ahmad, A Khursheed, et al. 2018. Community-based integrated approach to changing women's family planning behaviour in Pakistan, 2014–2016. *Public Health Action* 8, 2 (2018), 85–90.

[57] Mustafa Naseem, Fouzia Younas, and Maryam Mustafa. 2020. Designing digital safe spaces for peer support and connectivity in patriarchal contexts. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), 1–24.

[58] Unaiza Niaz. 2003. Violence against women in South Asian countries. *Archives of women's mental health* 6, 3 (2003), 173–184.

[59] Muhammad Jehanzeb Noor. 2004. *Daughters of Eve: Violence against women in Pakistan.* Ph. D. Dissertation. Massachusetts Institute of Technology.

[60] Fayika Farhat Nova, MD Rashidujjaman Rifat, Pratyasha Saha, Syed Ishtiaque Ahmed, and Shion Guha. 2019. Online sexual harassment over anonymous social media in Bangladesh. In *Proceedings of the Tenth International Conference on Information and Communication Technologies and Development.* 1–12.

[61] Roberta Liggett O'Malley and Karen M Holt. 2022. Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime. *Journal of interpersonal violence* 37, 1-2 (2022), 258–283.

[62] Unnati Patel and Ronald Roesch. 2022. The prevalence of technology-facilitated sexual violence: A meta-analysis and systematic review. *Trauma, Violence, & Abuse* 23, 2 (2022), 428–443.

[63] Ellen Pence and Michael Paymar. 1990. *Power and control: Tactics of men who batter: An educational curriculum.* Minnesota Program Development Incorporated.

[64] Emily Poole. 2015. Fighting back against non-consensual pornography. *USFL Rev.* 49 (2015), 181.

[65] Anastasia Powell and Nicola Henry. 2014. Blurred lines? Responding to 'sexting'and gender-based violence among young people. *Children Australia* 39, 2 (2014), 119–124.

[66] Erika Rackley, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn, and Anastasia Powell. 2021. Seeking justice and redress for victim-survivors of image-based sexual abuse. *Feminist Legal Studies* 29, 3 (2021), 293–322.

[67] Ahamed Sarjoon Razick, Mohammad Jazeel Mohammad Ibraheem, and Muhammadhu Ismail Nusrath Jahan. 2020. The significance of Mahar in Muslim marriages in Sri Lanka: a study based on Anuradhapura district. (2020).

[68] Scott Reeves, Ayelet Kuper, and Brian David Hodges. 2008. Qualitative research methodologies: ethnography. *Bmj* 337 (2008).

[69] Atta Ur Rehman, Rubeena Zakar, Muhammad Zakria Zakar, Ume Hani, Kamil J Wrona, and Florian Fischer. 2021. Role of the Media in Health-Related Awareness Campaigns on Perception of COVID-19: A Pre-post Study in the General Population of Pakistan. *Frontiers in Public Health* 9 (2021), 779090.

[70] Kristofer Rhude and Diane Moore. 2018. The third gender and Hijras. (2018). https://rpl.hds.harvard.edu/religion-context/case-studies/gender/third-gender-and-hijras

[71] David Ryan. 2018. European remedial coherence in the regulation of non-consensual disclosures of sexual images. *Computer law & security review* 34, 5 (2018), 1053–1076.

[72] Salams. 2023. Screenshot Prevention. (2023). https://faq.salams.app/en/articles/7868851-screenshot-prevention#

[73] Nithya Sambasivan, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Sanely Gaytán-Lugo, David Nemer, Elie Bursztein, Elizabeth Churchill, and Sunny Consolvo. 2019. " They Don't Leave Us Alone Anywhere We Go" Gender and Digital Abuse in South Asia. In *proceedings of the 2019 CHI Conference on Human Factors in Computing Systems.* 1–14.

[74] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. 2018. " Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018).* 127–142.

[75] Laura Savolainen. 2022. The shadow banning controversy: perceived governance and algorithmic folklore. *Media, Culture & Society* 44, 6 (2022), 1091–1109.

[76] Terri Schlichenmeyer. 2010. Wild West 2.0: How to Protect and Restore Your Online Reputation on the Untamed Social Frontier. *Network Journal* 17, 7 (2010), 46.

[77] Sarita Schoenebeck. 2022. Women's Perspectives on Harm and Justice after Online Harassment. *Jane Im, Sarita Schoenebeck, Marilyn Iriarte, Gabriel Grill, Daricia Wilkinson, Amna Batool, Rahaf Alharbi, Audrey Funwie, Tergel Gankhuu, Eric Gilbert, and Mustafa Naseem* (2022).

[78] Sarita Schoenebeck, Amna Batool, Giang Do, Sylvia Darling, Gabriel Grill, Daricia Wilkinson, Mehtab Khan, Kentaro Toyama, and Louise Ashwell. 2023. Online Harassment in Majority Contexts: Examining Harms and Remedies across Countries. *arXiv preprint arXiv:2301.11715* (2023).

[79] Sarita Schoenebeck and Lindsay Blackwell. 2020. Reimagining social media governance: Harm, accountability, and repair. *Yale JL & Tech.* 23 (2020), 113.

[80] Sarita Schoenebeck, Oliver L Haimson, and Lisa Nakamura. 2021. Drawing from justice theories to support targets of online harassment. *new media & society* 23, 5 (2021), 1278–1300.

[81] Sarita Schoenebeck, Carol F Scott, Emma Grace Hurley, Tammy Chang, and Ellen Selkie. 2021. Youth trust in social media companies and expectations of justice: Accountability and repair after online harassment. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–18.

[82] Martina Schwikowski. 2021. Africa mulls taxing Big Tech – DW – 02/12/2021. https://www.dw.com/en/africa-mulls-taxing-big-tech/a-56550570

[83] Silvia Semenzin and Lucia Bainotti. 2020. The use of Telegram for non-consensual dissemination of intimate images: Gendered affordances and the construction of masculinities. *Social Media+ Society* 6, 4 (2020), 2056305120984453.

[84] Chitrangada Sharma. 2018. REVENGE PORN: OFFENDING AND VICTIMIZATION IN DIGITAL AGE. (2018).

[85] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. 2018. Computer security and privacy for refugees in the United States. In *2018 IEEE Symposium on Security and Privacy (SP).* IEEE, 409–423.

[86] 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.

[87] Evan Stark. 2009. *Coercive control: The entrapment of women in personal life.* Oxford University Press.

[88] Statista. 2023. Number of social network users worldwide as of January 2023, by region. (2023). https://www.statista.com/statistics/454772/number-social-media-user-worldwide-region/

[89] Anselm Strauss and Juliet Corbin. 1990. Qualitative research. *Grounded Theory* (1990).

[90] Narendra Subramanian. 2008. Legal change and gender inequality: Changes in Muslim family law in India. *Law & Social Inquiry* 33, 3 (2008), 631–672.

[91] Sharifa Sultana, Mitrasree Deb, Ananya Bhattacharjee, Shaid Hasan, SM Raihanul Alam, Trishna Chakraborty, Prianka Roy, Samira Fairuz Ahmed, Aparna Moitra, M Ashraful Amin, et al. 2021. 'Unmochon': A Tool to Combat Online Sexual Harassment over Facebook Messenger. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems.* 1–18.

[92] Sharifa Sultana, François Guimbretière, Phoebe Sengers, and Nicola Dell. 2018. Design within a patriarchal society: Opportunities and challenges in designing for rural women in bangladesh. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems.* 1–13.

[93] Jeff R Temple, Hye Jeong Choi, Meagan Brem, Caitlin Wolford-Clevenger, Gregory L Stuart, Melissa Fleschler Peskin, and JoAnna Elmquist. 2016. The temporal association between traditional and cyber dating abuse among adolescents. *Journal of youth and adolescence* 45 (2016), 340–349.

[94] GEO TV. 2023. Kohistan honour killing case: Man accused of uploading doctored video on Facebook arrested. (2023). https://www.geo.tv/latest/522284-kohistan-honour-killing-case-man-accused-of-uploading-doctored-video-on-facebook-arrested

[95] Islam Uddin. 2018. Nikah-only Marriages: Causes, motivations, and their impact on dispute resolution and Islamic divorce proceedings in England and Wales. *Oxford journal of law and religion* 7, 3 (2018), 401–426.

[96] USEPA. 1990. Oil Spill Liability Trust Fund. (1990). https://www.epa.gov/oil-spills-prevention-and-preparedness-regulations/oil-spill-liability-trust-fund#:~:text=The%20Fund%20is%20administered%20by,connection%20with%20any%20single%20incident.

[97] Joris Van Ouytsel, Michel Walrave, Lieven De Marez, Bart Vanhaelewyn, and Koen Ponnet. 2021. Sexting, pressured sexting and image-based sexual abuse among a weighted-sample of heterosexual and LGB-youth. *Computers in Human Behavior* 117 (2021), 106630.

[98] Marco Viola and Cristina Voto. 2023. Designed to abuse? Deepfakes and the non-consensual diffusion of intimate images. *Synthese* 201, 1 (2023), 30.

[99] Jessica Vitak, Kalyani Chadha, Linda Steiner, and Zahra Ashktorab. 2017. Identifying women's experiences with and strategies for mitigating negative effects of online harassment. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing.* 1231–1245.

[100] Sebastian Wachs, Michelle F Wright, Manuel Gámez-Guadix, and Nicola Döring. 2021. How are consensual, non-consensual, and pressured sexting linked to depression and self-harm? The moderating effects of demographic variables. *International journal of environmental research and public health* 18, 5 (2021), 2597.

[101] Kate Walker and Emma Sleath. 2017. A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media. *Aggression and violent behavior* 36 (2017), 9–24.

[102] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L Mazurek, Manya Sleeper, and Kurt Thomas. 2022. Sok: A framework for unifying at-risk user research. In *2022 IEEE Symposium on Security and Privacy (SP).* IEEE, 2344–2360.

[103] Daricia Wilkinson and Bart Knijnenburg. 2022. Many Islands, Many Problems: An Empirical Examination of Online Safety Behaviors in the Caribbean. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems.* 1–25.

[104] JANIS WOLAK and DAVID FINKELHOR. 2016. SEXTORTION. (2016).

[105] Chin-Yuan Yeh, Hsi-Wen Chen, Shang-Lun Tsai, and Sheng-De Wang. 2020. Disrupting image-translation-based deepfake algorithms with adversarial attacks. In *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision Workshops.* 53–62.