LANDSCAPE ANALYSIS OF TECHNOLOGY-FACILITATED GENDER BASED VIOLENCE

Findings from the Asia Region

Prepared under Contract No.: GS-10F-0033M / 7200AA18M00016, Tasking N048
LANDSCAPE ANALYSIS OF TECHNOLOGY-FACILITATED GENDER BASED VIOLENCE

Findings from the Asia Region
FEVERUARY 2022

Prepared under Contract No.: GS-10F-0033M /7200AA18M00016, Tasking N048

Submitted to: Golnoosh Hakimdavar, USAID COR

Submitted by:

NORC at the University of Chicago
Vaiddehi Bansal, Mayumi Rezwan, Mithila Iyer, Kareem Kysia

International Center for Research on Women
Laura Hinson, Poulomi Pal, Erin Leasure, Connor Roth

Contractor:
NORC at the University of Chicago
4350 East West Highway, 8th Floor
Bethesda, MD 20814
Attention: Matthew Parry
Tel: 301- 634-5444; E-mail: Parry-Matthew@norc.org

DISCLAIMER

The authors’ views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

Recommended Citation:

NORC at the University of Chicago and the International Center for Research on Women (ICRW). Landscape Analysis of Technology-Facilitated Gender-Based Violence: Findings from Asia. 2022.
### TABLE OF CONTENTS

#### FIGURES
- Figure 1. Conceptual Framework for Technology-Facilitated GBV
- Figure 2. Geographic Distribution of Included Articles
- Figure 3. Flow Diagram of Literature Identification

#### ACRONYMS

#### EXECUTIVE SUMMARY

#### 1. INTRODUCTION
- DEFINITION AND SIGNIFICANCE

#### 2. METHODS AND LIMITATIONS

#### 3. FINDINGS, CONCLUSIONS AND RECOMMENDATIONS
- FINDINGS
- OVERVIEW OF TECHNOLOGY-FACILITATED GBV
- TECHNOLOGY-FACILITATED GBV TRENDS IN ASIA
- UNDERSTANDING THE CONTEXT OF TECHNOLOGY-FACILITATED GBV IN ASIA
- CHARACTERISTICS OF PERPETRATORS AND SURVIVORS
- IMPACTS OF TECHNOLOGY-FACILITATED GBV ON SURVIVORS
- HELP-SEEKING BEHAVIORS OF SURVIVORS
- RECOMMENDATIONS
- POLICY RECOMMENDATIONS FOR LOCAL/NATIONAL GOVERNMENT
- CONCLUSION

#### 4. REFERENCES

#### ANNEX A, RESEARCH QUESTIONS

#### ANNEX B, TERMS FOR SEARCH STRATEGY

#### ANNEX C, METHODS AND LIMITATIONS
### ACRONYMS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEC</td>
<td>Development Experience Clearinghouse</td>
</tr>
<tr>
<td>DRG-LER</td>
<td>Democracy, Human Rights, and Governance Learning, Evaluation, and Research</td>
</tr>
<tr>
<td>FGD</td>
<td>Focus Group Discussion</td>
</tr>
<tr>
<td>GBV</td>
<td>Gender-Based Violence</td>
</tr>
<tr>
<td>ICRW</td>
<td>International Center for Research on Women</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>KII</td>
<td>Key Informant Interview</td>
</tr>
<tr>
<td>LGBTQI+</td>
<td>Lesbian, Gay, Bisexual, Transgender, Queer, and Intersex</td>
</tr>
<tr>
<td>NCII</td>
<td>Non-consensual Distribution/Dissemination of Intimate Images</td>
</tr>
<tr>
<td>NCRB</td>
<td>National Crime Records Bureau</td>
</tr>
<tr>
<td>NGO</td>
<td>Non-Governmental Organization</td>
</tr>
<tr>
<td>NORC</td>
<td>National Opinion Research Center</td>
</tr>
<tr>
<td>OCSE</td>
<td>Online Child Sexual Exploitation</td>
</tr>
<tr>
<td>RFP</td>
<td>Request for Proposal</td>
</tr>
<tr>
<td>SNS</td>
<td>Social Networking Service</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>USAID</td>
<td>United States Agency for International Development</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

Across Asia, and mirroring global trends, women are experiencing a high prevalence of technology-facilitated violence. The UN Broadband Commission’s Working Group on Gender reported in 2015 that “approximately 73 percent of women across the globe have been targeted or exposed to some form of violence online (e.g., threats, harassment, or stalking)” (Kumar, Gruzd, and Mai 2021). Technology-facilitated gender-based violence (GBV) is defined as any action carried out using the internet and/or mobile technology that harms others based on their sexual or gender identity or by enforcing harmful gender norms (Hinson et al. 2018). The purpose of this study was to conduct a rigorous analysis of existing evidence on technology-facilitated GBV in Asia and make actionable research, policy, and programming recommendations.

To capture the breadth of information available on technology-facilitated GBV, the research team conducted a comprehensive search of peer-reviewed (academic) and grey literature (reports, briefs, white papers, and USAID DEC documents). The initial scope of the review included Central Asia and the Pacific Islands; however, since the team found insufficient literature from those regions, the report focuses on South and Southeast Asia. In addition to this landscape analysis, the team also conducted four case studies on Bangladesh, India, Indonesia, and Thailand to research country-specific trends, experiences, implications, and interventions.

Our review revealed that technology-facilitated GBV in Asia constitutes a myriad forms of abuse, violence, and harassment in the information communication technology (ICT) sphere and is largely shaped by key societal norms and values as well as the ever-evolving technological landscape within the region. Cyberbullying, cyberstalking, defamation, image-based abuse, sexual harassment, doxing, gendertrolling, and hacking are some of the many forms of violence perpetrated via technology. Given the anonymous nature of the online space, which enables users to conceal and manipulate identities, it is difficult to accurately discern information about perpetrators, such as their gender, age, location, profession, and relationship to their targets. However, overwhelming evidence indicates that there is a gender and sexual identity-based component of who experiences technology-facilitated violence, as a result of which, women, girls, and LGBTQI+ groups are much more likely to be targeted. Those with intersecting marginalized identities -- religion, caste/ethnicity, low-income, younger age, and people with disabilities are more vulnerable to experiencing both online and offline violence, have longer-lasting impacts, and are less likely to share or report the experience.

Findings also indicate that technology-facilitated GBV has varying and long-lasting impacts, including physical, psychological, social, economic, and functional outcomes comprising everything from feelings of guilt and shame to rape, acid attacks, and social isolation. The most common forms of addressing the issue include changing online behaviors, such as shutting down relevant accounts and self-censorship. However, significant barriers inhibit reporting and help-seeking behaviors. For instance, most social media, networking, and online dating platforms have methods in place for users to report and flag online harassment, abusive content, privacy violations, and fake profiles. However, many articles found that survivors are overall dissatisfied with the response and prevention tactics of platforms. Common barriers to reporting on platforms included poor awareness of reporting mechanisms (Devika et al. 2019); perceptions that the platforms would not do anything (Pasricha 2016); and a perception that filing a report is cumbersome and complex (Buhkari 2014). Similarly, although local law enforcement and government authorities have instituted both policy and programmatic responses to address cyber
violence to varying levels of effectiveness, governments face many response and prevention challenges as they struggle to create cohesive laws and timely policies that capture the increasing avenues of technology-facilitated GBV. Definitions for the forms of technology-facilitated GBV in multiple countries are disjointed, outdated, or non-existent in the laws (Akter 2015; Chowdhury 2016; Halder 2017; Randhawa 2010).

At the community level, literature indicates that community settings like schools and workplaces lack support mechanisms for survivors and are underutilized in response and prevention against technology-facilitated GBV. Although academic institutions serve as important resources for children and youth, educators lack the knowledge and curriculum to teach students about online safety and cyberbullying prevention (Gurumurthy, Vasudevan, and Chami 2019). Additionally, few individuals turn to their families or greater community for support after experiencing technology-facilitated GBV due to embarrassment, lack of empathy, and fear of re-victimization. At the community level, gendered social norms and patriarchal structures create a stigma that leaves survivors with limited ability to report, either because they would not be taken seriously or because experiencing violence is seen as a private matter (Devika et al. 2019; Randhawa 2010).

Addressing technology-facilitated GBV in Asia requires collective action from multiple actors at the global, state, and local levels. The following recommendations are informed by findings from this landscape analysis, country-specific case studies in Bangladesh, India, Indonesia and Thailand, and key informant interviews with relevant stakeholders in the four countries. Some of these recommendations have been noted previously but are repeated in this report as they are necessary elements to addressing technology-facilitated GBV and have specific applications to Asia.

**POLICY RECOMMENDATIONS FOR LOCAL/NATIONAL GOVERNMENT**

- Conduct an analysis of the legal landscape from a survivor and human rights–centered lens.
- Enact laws specific to technology-facilitated GBV.
- Assess and amend/repeal anti-obscenity and anti-pornography laws that are actively harming survivors or restricting consensual sexual expression.
- Conceptualize and circulate clear definitions of and information about technology-facilitated GBV with law enforcement and legal officials.
- Increase capacity for existing independent state bodies/organizations with a focus on technology-facilitated GBV.
- Repeal transphobic and homophobic legislation and strengthen protections for the LGBTQI+ population.

**PROGRAMMING RECOMMENDATIONS FOR LOCAL/NATIONAL GOVERNMENTS AND CIVIL SOCIETIES**

- Conduct public education campaigns on technology-facilitated GBV.
- Develop specialized training for law enforcement and legal officials.
- Enhance data collection by streamlining reporting processes for survivors.
• Launch digital literacy and online safety training.

RECOMMENDATIONS FOR TECHNOLOGY COMPANIES
• Enhance privacy settings of digital platforms.
• Review online community standards to ensure gender and context are taken into consideration.
• Strengthen staff capacity to improve response mechanisms and support resources.
• Invest in trauma-informed and transparent reporting and response mechanisms.

RECOMMENDATIONS FOR RESEARCHERS
• Increase focus on Central Asia and Pacific Islands.
• Strengthen research partnerships with those responsible for reporting mechanisms and data collection.
• Investigate social media’s role in facilitating and addressing technology-facilitated GBV.
• Increase knowledge of survivor-centric and culturally-nuanced responses.
• Examine the gendered impact in areas or sectors with burgeoning technology growth.
• Investigate trauma-informed best practices between employers and employees.
I. INTRODUCTION

Under the Democracy, Human Rights, and Governance Learning, Evaluation, and Research (DRG-LER) II Activity, the United States Agency for International Development (USAID) contracted NORC at the University of Chicago (NORC) in partnership with the International Center for Research on Women (ICRW), to conduct a landscape analysis comprising a systematic evidence review and case studies to understand technology-facilitated gender-based violence (GBV) in Asia.

There is growing interest among implementers and policy-makers to address this growing global issue that, although widespread, has inconsistent terminologies and perceptions of what constitutes various forms of GBV behaviors perpetrated through users of technology. Moreover, there has not been a similar review of the Asia region to examine the numerous components of technology-facilitated GBV, regional and gender differences, interventions and their evaluations, and response mechanisms. The purpose of this study was to conduct a rigorous analysis of existing evidence of technology-facilitated GBV in Asia, summarize key gaps in the current knowledge base, and make recommendations to inform future research and programming.

DEFINITION AND SIGNIFICANCE

Technology-facilitated GBV is defined as any action carried out using the internet and/or mobile technology that harms others based on their sexual or gender identity or by enforcing harmful gender norms (Hinson et al. 2018). Perpetrators and survivors can be of any gender, and the rationale behind the violence is often rooted in hateful and hurtful actions based on someone’s sexual or gender identity. However, despite knowing all of this, it can at times be difficult to define clear-cut cases of technology-facilitated GBV.

The evidence-based conceptual framework below (Figure 1) outlines an experience of technology-facilitated GBV, from the motivations and intentions of perpetrators to the impacts and help-seeking behaviors of survivors. It focuses on six tactics that cross-cut various violent behaviors, including doxing, hacking, threatening, image-based abuse, gendertrolling, and use of fake accounts.
The UN Broadband Commissions for Digital Development Working Group notes that technology-facilitated GBV is a growing international phenomenon. Global literature also indicates that this type of violence:

- Is often connected to offline violence
- Impacts women, girls, and the LGBTQI+ community at disproportionately higher rates (survivors\(^1\) of technology-facilitated GBV are not only targeted because of their female-identify but may experience violence because of their gender identity or sexual orientation as well)
- Contributes to the gender digital divide\(^2\) and
- Suppresses rights and civic participation, especially for women and girls

All of these aspects—singularly or together—can have catastrophic implications not only for women, girls, and the LGBTQI+ community but also for societies.

---

\(^1\) Note on terminology: Report authors primarily use the term “survivor” in this report, as it is more empowering than “victim” and has become standard in the GBV field. The exception to this is when a statement implies that an individual is being processed through the criminal justice system or is currently experiencing violence, in which case they are referred to as a “victim.”

\(^2\) The digital divide is the distinction between those who have internet and/or mobile access and are able to make use of digital communications services, and those who are excluded from these services. The gender digital divide reflects the inequalities between men and women in terms of digital technology access and use.

2. METHODS AND LIMITATIONS

The research team developed priority research and sub-research questions in collaboration with USAID to guide the research process (Annex A). Given the paucity of evidence on this nascent topic, the research questions focused on descriptive categories, such as trends, profiles of survivors and perpetrators, the impacts of experiencing such violence and harassment, and challenges to and facilitators of help-seeking behaviors.

To capture the breadth of information available through a growing body of evidence, the research team conducted a comprehensive search of peer-reviewed (academic) and grey literature (including program documents, white papers, and USAID DEC documents). The research team began with a definition of and conceptual framework for “technology-facilitated GBV” developed by ICRW (Figure 1). From this, the research team organized key concepts into a table of searchable terms (Annex B), which informed both the peer and grey literature search strategies. The initial scope of the review included Central Asia and Pacific regions; however, as the team found insufficient literature from those regions, the focus of this report is on South and Southeast Asia.

In total, the team screened over 2,000 articles and then analyzed 97 articles as part of the final included set. Annex C presents additional details about the methodology behind the literature review process. Figure 2 below shows the geographic distribution of articles included in the study.3

Figure 2. Geographic Distribution of Included Articles

---

3 Some articles included in the review reported on multiple countries and were therefore double-counted in the graph.
3. FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

FINDINGS

OVERVIEW OF TECHNOLOGY-FACILITATED GBV

Technology-facilitated GBV constitutes a myriad forms of abuse, violence, and harassment in the information communication technology (ICT) sphere, including the use of devices and platforms such as mobile phones, social media, and the internet. The overwhelming majority of evidence indicates that there is a gender and sexual identity-based component of technology-facilitated violence, as a result of which, women, girls, and LGBTQI+ groups are much more likely to be targeted. However, the internet can be used as both a tool of empowerment and as a means of harassment; Hassan et al. (2018) highlight this contrast in their study that examines the usage of social media campaigns to counter sexual harassment and the presence of social media websites as a mechanism for perpetrating violence. The nebulous nature of this harassment through online platforms can cause severe detrimental impacts on women’s physical, psychological, and financial well-being in addition to societal stigmatization due to the challenges associated with its prosecution—among other offline consequences, such as decreased social media presence and inhibited freedom of expression socially (Halder 2017; Gurumurthy, Chami, and Vasudevan 2017).

Understanding the nature of technology-facilitated GBV requires special attention because it is different from that of offline harassment, as online platforms afford a vast degree of anonymity that offline interactions do not (Digital Rights Foundation 2017). Further, similar to in-person violence, the positive and negative aspects of ICT and its associated use for the perpetration of technology-facilitated GBV are strongly related to the cultural context of its country of usage (Hassan, Unwin, and Gardezi 2018).

RELATION BETWEEN ONLINE AND OFFLINE VIOLENCE

Findings from Asia suggest that technology-facilitated GBV and offline violence are often interlinked and cannot be separated (Devika et al. 2019; UN Women 2020; Datta 2013):

“Cyber violence [in India] was not understood as something separate from physical violence but an extension of it by the women survivors.” —Sarkar and Rajan (2021)

Experiencing violence offline after experiencing online violence appears to be common in some contexts, including in Thailand, where nearly 70 percent of those who had been victimized online were also victimized offline (Ojanen et al. 2015). In other examples, victims of online violence and harassment end up getting harassed in the streets or even raped and murdered:

“Out of all the crimes described by the respondents, teenage girls being sexually harassed and raped tops the list. These cases occur because they use social media such as Facebook to communicate with strangers. Typically acquainted via social media, they would later be asked to meet in real life and this would sometimes lead to … out of wedlock pregnancy” —Ghazali and Ghani (2018)

“Aside from inflicting very real psychological injury, targeted online violence poses increasing physical safety risks, especially in the context of campaigns against women journalists that trigger mob reactions. One tenth (20 percent) of the women journalists we surveyed [in 15 countries, including
Some in Asia reported experiencing abuse and attacks in the physical world that they believe were seeded online. This ending is particularly disturbing given the emerging correlation between online attacks and the actual murder of journalists with impunity.” –Posetti et al. (2021)

Below, the research team provides overviews of the different forms of technology-facilitated GBV that appeared frequently in this review. As different forms of technology-facilitated GBV often overlap, it is important to note that the categories are not mutually exclusive. Those overlaps are described where possible in the rest of this section.

**CYBERBULLYING OR ONLINE BULLYING**

Cyberbullying is defined as “an aggressive and intentional act that is carried out using electronic forms of contact by a group or an individual repeatedly and over time against a survivor who cannot easily defend him or herself” (Khine et al. 2020). The literature from Asia presents several variations of this definition, all highlighting the repetitive and targeted nature of this form of violence (Bhat et al. 2017; Khine et al. 2020; Haarr 2013). This form of technology-facilitated GBV involves primarily male perpetrators bullying female targets, though male perpetrators have also been found to harass others of their own gender (Adebayo et al. 2020; Musharraf et al. 2019; Bhat 2017). Motivations behind gender-based cyber-bullying include defamation, sexual harassment, and hate speech.

Existing evidence indicates that cyberbullying has become more common than offline harassment in Asian countries such as Thailand (Ojanen et al. 2015). In a 2012 study conducted by Microsoft, India ranked third among 25 countries in instances of cyberbullying, with approximately 50 percent of young and adolescent Indian internet users having experienced cyberbullying (Jain and Agrawal 2020), and Malaysia ranked 17th highest (Balakrishnan 2015). Another recent study found that 3 in 10 Malaysian youths have been victims of online violence or bullying (Fitriana, Souket, and Yie 2020). In Vietnam, the “rapid and widespread development of the internet and technology facilities such as computers, mobile phones” have shown an increase in students experiencing cyberbullying, and nearly 31 percent of junior and senior high school students have been targets of cyberbullying (Q. T. Le 2020). Similarly, in Pakistan, cyberbullying and harassment amount to 32 percent of all cybercrimes reported in the country (Saleem, Khan, and Zafar 2021). Another recent study in Thailand found high cases of abuse and harassment perpetrated through the internet and mobile phones in regions with relatively lower tech usage but with high community violence rates, indicating that violence rates can be magnified through use of internet and mobile phones (Pradubmook-Sherer and Karansupamas 2020).

While it is an increasingly common form of technology-facilitated violence, the gendered nature of cyberbullying is not consistent across the literature. Although some studies have found that cyberbullying involves primarily male perpetrators bullying female targets (Adebayo et al. 2020; Musharraf et al. 2019; Bhat 2017), others have reported no gender differences in cyberbullying victimization (Balakrishnan 2018; Saleem 2021). For instance, in Malaysia, Adebayo et al. (2020) found that among high school and undergraduate students, boys and young men are the primary perpetrators of cyberbullying, and Fitriana et al. (2020) found that Malaysian men are also more likely to be victims of traditional bullying and cyberbullying (Adebayo, Ninggal, and Bolu-Steve 2020; Fitriana, Souket, and Yie 2020). Similarly, in India, there is no consistent correlation between gender and cyberbullying perpetration: while Bhat et al. (2017) found that boys were more likely to engage in cyberbullying than girls, Sharma et al. (2017) found that women were found to be active perpetrators of cyberbullying.
DEFAMATION

Defamation in the context of technology-facilitated GBV can take place through dissemination of false information or altered images via email, posts on social media platforms, messages in online public fora, mailing lists, and bulletin boards (Datta et al. 2020) and is used to target survivors with the purpose of damaging their reputations. Ghazali and Ghani (2018) note that the risk of defamation is a factor that inhibits some survivors from freely expressing opinions and posting images while curating their social media presence, as “social media is rife with slanders purposely uploaded to tarnish peoples’ image.” Survivors also report fear of using internet platforms and social media sites like Facebook, as they are afraid perpetrators might slander their presence, and they might become the target of further online harassment, stalking, and defamatory posts. Research suggests that high-profile celebrities; those in public roles, such as politicians or journalists; younger individuals; school students; and individuals from marginalized groups, such as Dalit women in India, are most frequently the target of vitriolic defamatory attacks online (Kumar, Gruzd, and Mai 2021; Kunbuddee et al. 2021; Gurumurthy 2019).

SEXUAL HARASSMENT

Sexual harassment in the context of technology-facilitated GBV includes unwelcome sexual advances, requests for sexual favors, and other verbal or physical harassment of a sexual nature, perpetrated through online or technological means. Prevalent “eve-teasing”—a common euphemism in South Asia for sexual harassment of women in public places by men (Talboys et al. 2017)—can normalize online sexual harassment as a consequence of the offline world (Koirala 2020). However, it severely impacts the online presence of survivors, often leading them to reduce or stop usage of a certain platform or social media site.

In a study by Nova et al. (2019), the majority of Bangladeshi women participants complained about being sexually harassed over social media, receiving messages that were categorized as either sexual prepositions, sexually objectifying contents, romantic messages, or dating inquiries. A study in Pakistan found that direct messages and phone calls were the most frequent modes of sexual harassment (Hassan, Unwin, and Gardezi 2018). Sambasivan et al. (2019) similarly note that many South Asian women also experienced cyber harassment through unwanted phone calls and text messaging.

The prevalence of experiencing online sexual harassment depends on factors such as age and profession. In Nepal, despite recent increase in the number of woman journalists since the end of armed conflict in 2006, there continues to be widespread gender-based discrimination and online harassment that “[pose] an additional threat to the participation of women in a male-dominated profession such as journalism” (Koirala 2020). In a study sample of 46 Nepali female journalists, 82 percent of female journalists in the 21–25 age group were more likely to have experienced online sexual harassment, compared to 50 percent of women journalists above age 35. Journalists in junior positions were also more likely to face abuse online than their senior counterparts. This gendered harassment reflects that widespread discrimination against women in Nepali society is also being depicted online (Koirala 2020).

Though sexual harassment is a high-incidence crime, underreporting and a lack of willingness to report the crime may hide the true extent of the issue in Asia. For example, while India’s National Crime Records Bureau (NCRB) recorded that only 10 percent of cybercrimes reported in 2014–15 were related to offenses against women or of a sexual nature, Gurumurthy, Vasudevan, and Chami (2018) suggest that official statistics may not give a full picture, as the majority of victims of technology-facilitated GBV do not seek legal recourse. A 2016 survey in India found that although 58 percent of a
sample of 500 individuals reported facing some form of online harassment, 38 percent of them did not take any action (Gurumurthy, Chami, and Vasudevan 2017). Saleem, Khan, and Zafar (2021) note similar findings among participants in their study in Pakistan, where 62.2 percent of females said they never reported when they received threatening messages of a sexual nature; a similar proportion of men also never reported threatening messages online. Marret and Choo (2017) note in their study that in Malaysia, the higher prevalence of online harassment compared with unwanted sexual solicitation resembles the pattern of offline victimization, where levels of physical and psychological victimization exceed sexual victimization.

CYBERSTALKING

Cyberstalking is a highly intrusive mechanism for gaining information about survivors through repeatedly initiating unwanted contact for the purposes of defamation, sexual harassment, and other forms of exploitation. It is a severe form of cyber harassment that constitutes a credible threat of harm to the target (PEN America 2021). Cyberstalking is also one of the most reported forms of technology-facilitated GBV in India, with 66 percent of women, especially younger women, experiencing cyberstalking incidents (Xu 2010). Among participants in Sambasivan et al.’s 2019 study, cyberstalking was the most common form of abuse reported in Bangladesh, Pakistan, and India, with some women reportedly experiencing it on a daily basis. The researchers also noted that cyberstalking is particularly dangerous, as perpetrators find potentially identifying information, such as addresses, and can then use the information to stalk their targets both online and in-person (Sambasivan et al. 2019).

ONLINE EXPLOITATION AND CYBERGROOMING

Online sexual exploitation is a rampant form of abuse. Increased time spent online during the COVID-19 pandemic has rendered several at-risk groups, such as children, teenagers, and young women, particularly vulnerable to perpetrators (Gill 2021). This form of exploitation can manifest in numerous ways, such as through the order of “mail order brides” using internet services in Malaysia (Leng et al. 2014); posting deepfakes (images, audio, or video created using artificial intelligence to superimpose an individual’s face on videos or images to create fake pornography) in cases from India (Haldar 2017); or the facilitation of trafficking through the dissemination of explicit images (Flynn 2019, Randhawa 2010; Dunn 2020). Perpetrators may also threaten survivors by blackmailing them for money or other goods if they do not want offensive material to be leaked (Sambasivan et al. 2019).

Cybergrooming is a particularly grave form of exploitation, as there is typically an age differential between the perpetrator and survivor and it involves someone (often an adult) who befriends or forms a close connection with a minor online with ultimate intentions of sexual abuse, sexual exploitation, or trafficking (ChildSafeNet, n.d.). The internet provides anonymity to perpetrators, who befriend their targets in order to coerce them into sharing graphic or sexually explicit photos of themselves or even to lure them into unwanted sexual activities (Chowdhury 2016). It is perpetrated to gain the trust of targets, who then may be subjected to other offline forms of violence such as harassment and stalking, with the ultimate objective of exploitation and abuse. The timespan of this form of violence can range from a few short weeks to several years (Andrews et al. 2020). Wachs et al. (2016) conducted a study reporting the prevalence of cybergrooming across Germany, the United States, the Netherlands, and Thailand, in which the data indicated that participants in Western nations exhibited lower risk for experiencing cybergrooming compared to Southeast Asian participants. The authors suggest that these differences might be explained by reduced monitoring of online activity by parents, as well as
cultural differences such as sensitivity to sexual aggressions online and poor parent-child communication. The authors also note that prevalence for cybergrooming is difficult to measure due to limitations of self-reports, police reports, and law enforcement interviews.

Cybergrooming is also closely linked to the online child sexual exploitation (OCSE), a growing form of online abuse where minors are coerced into sexual activity. Online platforms may be used to exploit targets for the intention of trafficking, with certain platforms, such as online chat rooms, advertisements for employment, marriage agencies, and dating agencies, used to lure survivors. The Philippines is considered a “hot spot” for OCSE, with cases rising each year. According to a recent report, the Philippines government recorded 280,000 cases of cybersex trafficking or the online streaming of sexual abuse of children in 2020 (Save the Children and Plan International 2020).

Finally, the International Organization for Migration (IOM) found that most survivors of trafficking solicited or exploited through the internet come from Asia, “with more than 225,000 arriving annually from Southeast Asia and more than 150,000 from South Asia” (Leng, Khan, and Rahim 2014). Additionally, in India, the sale and exchange of “rape videos” online is a particularly disturbing and increasing trend. Entire websites are dedicated to “rape pornography,” driving an increase in incidences of cybersex trafficking for these purposes and in production of more videos of sexual assault (Dunn 2020). According to research in Southeast Asian countries, a combination of poverty and expanding internet infrastructure are contributing factors to the expansion of trafficking and related abuse, such as cyber prostitution (Brazal 2020).

HATE SPEECH

Hate speech in the context of technology-facilitated GBV encompasses insults or attacks against targets based on their gender, sexual identity, or presentation, or derogatory speech toward protected groups through use of technology (Kumar et. al 2021). In the online sphere, the term “speech” expands to include targeted text, images, and videos, in addition to voice calls.

Online hate speech is commonly directed toward populations, and especially women, who belong to religious or ethnic minorities or who hold views that do not align with social norms or existing political scenarios in the country of origin (Chowdhury 2016). Islamophobic hate speech that falls within the technology-facilitated GBV space appears particularly ubiquitous, with survivors in India facing vitriolic name-calling such as “Jihadi Jane” (Rae 2020). In India, caste-based discrimination against women is also prevalent online, with the perpetrators often being of higher castes (such as Brahmins) than their targets (Munusamy 2018). Sources in Asia also highlight the public nature of social media as a key driver of online hate speech, where women who are politically active on social media may be particularly targeted with online hate speech “so that people can see it” (Chowdhury 2016). One study from Indonesia found that social media channels like Facebook or Twitter are used by people to express homophobic sentiments (Mana, Wahyuni, and Baadila 2015).

DOXING

Doxing is a form of technology-facilitated GBV that involves the malicious disclosure of private or identifying information (such as addresses, government identification numbers, employment details, family information) about anonymous individuals on the internet (Sambasivan et. al 2019). It is also commonly associated with threatening, sexual harassment, and other forms of directed abuse used to shame survivors. In Pakistan, Hassan et al. (2018) found that in cultures where pre-marital interactions
between genders is stigmatized, some men harass and threaten their ex-girlfriends after breakups by posting or sharing identifying information and pictures online.

Reports from Asia indicate high incidents of content leaks and/or doxing. Amnesty International found that in 2018, one-third of women in India who experienced online harassment had been doxed (Dunn 2020). LGBTQI+ populations are especially at risk of being doxed by perpetrators who wish to out them. This can often be through events they attend where identifying information is circulated about them later or by meeting someone online who later outs them. Doxing can thus severely impact the physical safety and mental health of these groups (Chowdhury 2016; Bhattacharjya et al. 2011; Dunn 2020). This is corroborated in Sambasivan et al.’s (2019) study in Bangladesh, Pakistan, and India, where survivors reported experiencing physical violence as a consequence of online abuse—both from perpetrators of online abuse as well as from family members.

**Hacking**

Hacking is another prevalent form of cyber violence against women and girls (Halder 2017). Hacking of survivors’ data occurs through the usage of technology to access accounts without permission and is most perpetrated through the internet and social media sites. For example, in Bangladesh, hacking is used to commit other forms of gender-based abuse, such as sexual harassment, image-based abuse, or defamation, with photos or identifying information leaked from survivors’ profiles (Akter 2018).

Panchanadeswaran et al. (2017) found in their study in India that targets of hacking were at risk of physical or intimate partner abuse as a result of constant monitoring, as the information such as internet search history or real-time locations gleaned through hacking enabled perpetrators to commit offline violence against their partners in some cases.

**Threatening Behaviors**

Threatening behaviors in the context of technology-facilitated GBV include the expression of statements intended to inflict pain, injury, damage, or other hostile action through various means of communication, such as social media, email, phone calls, or SMS. It may manifest in several forms, such as physical, sexual, or escalated violence online, and could be targeted toward a specific individual or include their family and social circle. Coercive sexting or sexual harassment includes pressure to send sexually explicit text communication, including images or messages (Hassan, Unwin, and Gardezi 2018).

Online threatening behaviors often also go hand in hand with blackmail. Findings from Pakistan indicate that cyber harassment, threats of offline violence, and blackmail of nonconsensual dissemination of images are forms of harassment commonly faced by women on social media, due to aggravated patriarchal cultural norms that do not align with women using social media (Aksar et al. 2020). Another study from Pakistan indicates that intimate partners leak images or sexually harass women by threatening and demanding favors, money, or re-engaging in previous romantic relationships after breakups (Hassan, Unwin, and Gardezi 2018).

**Image-Based Abuse**

Another pervasive form of technology-facilitated GBV in Asia is image-based abuse, which constitutes creating, altering, obtaining, using, distributing, or threatening to distribute non-consensual, intimate, sexual, or personal images (McGlynn and Rackley 2017). Non-consensual distribution of intimate images
(NCII) refers specifically to the distribution of private or sexually explicit images or videos of individuals without their consent (PEN America 2021). NCII is a highly gendered phenomenon often perpetrated by men, who request intimate information and photos after gaining the trust of their partner (Dunn 2020). Image-based abuse in Asia can include synthetic porn, such as superimposing women’s faces on pornographic images (Sambasivan et al. 2019), or instances where survivors are sent obscene images or videos (Chen et al. 2020).

“Deepfakes” are images, audio, and/or video that are created using a form of artificial intelligence to appear real, which can be used to superimpose an individual’s face to videos or images to create fake pornography. When these are created, distributed, or threatened to be distributed without the consent of the person whose face appears, it is considered a form of image-based abuse (Flynn 2019). In one study, researchers found that 96 percent of total deepfake content found online was pornographic in nature (as opposed to non-pornographic content). Most of the women who appeared in these deepfakes did not consent to their images being used (Dunn 2020). Sambasivan et al.’s 2019 study from South Asia found that six percent of participants reported experiencing synthetic porn (Sambasivan et al. 2019).

The capability to take and share images via mobile phones also allows perpetrators to use images to coerce and harass women. A cross-country study from Malaysia, Cambodia, Pakistan, and the Philippines highlights that the ability to widely disseminate intimate images through online platforms is a factor that allows perpetrators to blackmail and shame targets, for purposes ranging from remaining in romantic relationships with existing intimate partners or sharing images of well-known public figures and actresses (Randhawa 2020). A study on sex workers in India also found that some respondents faced “clients attempting to violate their sense of privacy through non-consensual stealth photography and video recording” (Panchanadeswaran et al. 2017).

**GENDERTROLLING**

Gendertrolling consists of mobilizing a group of individuals across online platforms to target individuals active in social media and online spheres (Kumar et al. 2021). This mass-organized act of misogynistic online violence is usually perpetrated by male-identifying strangers who come together to intimidate and overwhelm the targeted individual through insults, slurs, and threats of violence (Gurumurthy, Vasudevan, Chami, and Mahesh 2019). This form of violence is closely linked with sexual forms of harassment, including defamation and public shaming of women for assumed sexual activity or experiences. According to the literature reviewed, there are several factors that play into this form of abuse in Asia, including religion, ethnicity, and profession. Reports from India suggest that trolls from conservative Hindu nationalist parties target women they feel are “corrupted by technologies” and publicly shame them in the digital realm (Arora and Scheiber 2017; Kumar, Gruzd, and Mai 2021). Another report in India notes that trolling based on caste or minority religious identity is often accompanied by “sexualized, gender-based trolling” (Gurumurthy, Vasudevan, Chami, and Mahesh 2019).

Targets of gendertrolling in Asia tend to be associated with certain public-facing professions, such as activism, academia, journalism, or politics. For example, Indian journalists were subjected to increased trolling after reporting on sensitive issues such as politics or region (Chen et al. 2020; Gudipaty 2017).
**USING FAKE ACCOUNTS**

The creation of fake accounts within online communities for the purpose of trolling or obtaining information to be used for exploitation or arrest is a tool used for technology-facilitated GBV. This form of violence manifests primarily as a precursor to others, such as trolling, doxing, harassment, and defamation, with this form of abuse extending to larger and more prominent figures, such as female politicians and journalists who—due to their significant online presences—are often targeted by several users of fake accounts (Halder 2017). In Hyderabad, India, the use of fake accounts to extract money is so commonplace that police have set up a website for users to detect and protect themselves from such deception (Arora and Scheiber 2017). While survivors in Bangladesh express desire to press charges against their harassers, the systems in place to address this abuse often lack the technical capacity to move forward with such cases (Nova et al. 2019). Beyond the clear monetary damage resulting from this form of fraud, victims suffer psychological impacts of experiencing such deception and exploitation.

The use of fake profiles is an increasing concern in Malaysia, especially in the context of romance fraud or “online love scams,” which was the highest form of cyber fraud reported in the country in 2020 (Kamaruddin et al. 2020). This form of deception tends to have exploitative intentions, where scammers befriend and defraud Internet users of large sums of money, while also causing psychological damage (Arora and Scheiber 2017). Reports indicate that “an average of seven people in Malaysia [are] falling victim to ... love scams per day.” While most targets of romance fraud are lonely and elderly women, the number of Generation Y and Millennials targets is growing. In 2019, romantic scams cost a total of 68 million ringgit (approx. 16,229,116 USD) (Kamaruddin et al. 2020).

**VIOLENT EXTREMISM**

Although not a well-defined aspect of this form of violence, the intersection of violent extremism and technology-facilitated GBV is important to understand, given some findings that religious and political minorities are at higher risk of harm. Violent extremism on technological platforms arises through the broadcasting of views linked with ideologies associated with extremism, inciting violence and radicalism. Extremist views stated online often aim to amplify existing communal prejudices and increase online violence against vulnerable groups, as this form of violence is most frequently aimed at targets with intersectional identities.

Research conducted for this report yielded only three articles that mention violent extremism in the context of technology-facilitated GBV in Asia, suggesting that this is an area of research that is still new and contains knowledge gaps. This literature also suggests that violent extremism manifests in combination with other forms of technology-facilitated GBV, such as gendertrolling, doxing, and—most particularly—hate speech. Review of the articles available indicates that religious minorities are at notably higher risks of targeted violent extremism as a form of online abuse. Communal tensions in certain countries could indicate motivations of perpetrators in committing this type of violence, as indicated by the following excerpt, which highlights gendertrolling faced by religious minorities in India:

“A friend got trolled during elections since she is a Muslim [minority section in India]…. [She] was asked to move to Pakistan.” —Gudipaty (2017)

Johnston et al. (2020) indicate that terrorist organizations such as the Islamic State frequently use online platforms such as Twitter to target individuals, recruit members, and spread extremist views. In
addition, these findings show that women from these groups might also be perpetrating violence against other women through the imposition of extremist religious views.

“Terrorist groups in Pakistan with a women’s outreach wing have far more supporters than groups without…. Women are interested in extremism, with women accounting for 33 percent of those searching the internet for violent extremist material. Moreover, 80 percent of the 670,000 searches for extremist material across four Asian countries (Bangladesh, Philippines, Malaysia, Indonesia) over a two month period in 2018 were from Indonesia.”—Johnston et al. (2020)

TECHNOLOGY-FACILITATED GBV TRENDS IN ASIA

While many studies in this review shed light on the prevalence of technology-facilitated GBV in Asia, it is difficult to estimate nationally representative prevalence rates for individual countries due to factors such as underreporting, poor reporting mechanisms, and a lack of understanding of what constitutes forms of technology-facilitated GBV that can be reported (Office for Victims of Crime Training and Technical Assistance Center n.d.; Hassan, Unwin, and Gardezi 2018). Findings also indicate that prevalence varies by the form or behavior of technology-facilitated GBV, as well as characteristics of both the survivor and perpetrator (International Foundation for Electoral Systems 2019).

While a common trend of increasing technology-facilitated GBV can be observed across the region, individual country contexts drive how, why, and for whom prevalence is increasing over time. For example, in India, the prevalence of technology-facilitated GBV is increasing, with women, girls, and LGBTQI+ individuals experiencing disproportionate impacts (Quilt.AI and ICRW 2021). One source connects increased violence, especially against journalists and women from marginalized caste groups to political change and the rise of Hindu nationalism since 2014 (Pasricha 2016). In Bangladesh, women are disproportionately targeted by online violence and harassment, which has increased particularly as expansion of the ICT sector and growing internet penetration have overlapped with existing sociocultural contexts and inadequate legal protections (Akter 2018). In Indonesia, there was a particular rise in anti-LGBTQI+ rhetoric in social media between 2016–2017, which is attributed to a range of factors, including the political environment and an increased publicity of events in media (Boellstorff 2020). Brazal (2020) indicates that in Southeast Asian countries such as the Philippines, Cambodia, and Indonesia, poverty and expanding internet infrastructure has given rise to an industry of cyber prostitution, especially of minors (Brazal 2020).

COVID-19 PANDEMIC

The COVID-19 pandemic has particularly impacted trends and prevalence of technology-facilitated GBV globally and across countries in Asia. In India, increased concern over online violence during the pandemic is evidenced by increasing conversations around online GBV on Twitter, which nearly tripled during the 2020–2021 period of COVID-19 compared to before. In addition, authors found an uptick in searches for help-seeking behaviors related to technology-facilitated GBV in some regions during that same pandemic period, as compared to before the pandemic (Quilt.AI and ICRW 2021).

Users with limited digital skills, who are more likely to be women and girls, are at higher risk of cyberviolence during COVID-19 as they may not have access to the knowledge and best practices for online protection. Children are especially at high risk, as more time online to access education and entertainment during quarantine has led to increased exposure to cyberbullying, harmful content, and
exploitation. Further, children whose parents are less technologically savvy are at particular risk due to weakened parental oversight, advice, and guidance. Additionally, economic pressure on families as a result of the pandemic increases the potential for exploitation of girls for economic gain (Save the Children and Plan International 2020). A report by UN Women (2020) notes that these impacts of COVID-19 reflect a larger context of gender-based discrimination and violence globally:

“ICT facilitated violence has spread under the shadow pandemic of violence against women. During COVID19, violence against women is manifested in different forms, including … online and ICT-facilitated violence. These forms of violence and abuse take place in a context of wide-spread systemic gender-based discrimination…. During COVID, as more women use the internet and social media to advocate for their rights in open links and public debates there is a higher risk to be targeted.” –UN Women (2020)

UNDERSTANDING THE CONTEXT OF TECHNOLOGY-FACILITATED GBV IN ASIA

Myriad contextual factors facilitate technology-facilitated GBV. The reviewed literature indicates that technology-facilitated GBV in Asia is largely shaped by key societal norms and values as well as the ever-evolving technological landscape within the region.

SOCIOCULTURAL CONTEXT

Key societal factors relevant to technology-facilitated GBV in the Asia region include: patriarchal social norms, familial power dynamics, taboos surrounding sex and sexuality, and normalization of GBV.

According to a recent study, motivations behind technology-facilitated GBV are more apparently observed in male-dominated communities (Kumar, Gruzd, and Mai 2021), and findings from South Asia particularly indicate that deeply embedded gender inequalities and patriarchal norms contribute to the increased risk women face of being targeted online (Gurumurthy, Vasudevan, and Chami 2019; Posetti et al. 2021; Gurumurthy, Vasudevan, Chami, and Mahesh 2019; Digital Rights Foundation 2017). For instance, Pakistan has been described as a patriarchal and highly religious society, in which traditional cultural values play a strong role in shaping an individual’s identity and behavior online (Hassan and Unwin 2017). Similarly in Nepal, sexism is normalized and replicated online, with behaviors such as posting sexist jokes and comments considered acceptable (Koirala 2020).

Familial and kinship dynamics also shape the context of technology-facilitated GBV in Asia. Parents’ concern on children’s use and risk of technology can often be influential in shaping public discussion and views. For example, in 2018, police in Tamil Nadu, India, issued advisories to parents about using TikTok as there were reports that photos of women were being downloaded from the app and being altered for nefarious use. This led to what the source describes as a “moral panic and outrage in public discourse about the use of the app, prompting the police to issue a ban that was subsequently struck down”(Gurumurthy, Vasudevan, and Chami 2019). Parents in India are also concerned about the use of cyber cafés by children to circumvent restrictions placed at home, as well as about the effects of normalized GBV in online games (Bhattacharjya et al. 2011).

Varying levels of digital literacy among parents may weaken their ability to provide guidance and oversight on computer and internet use and has been found to be associated with increased risk of exposure among children and adolescents to cyberbullying, harmful content, and sexual exploitation
(Save the Children and Plan International 2020; Musharraf et al. 2019). Additionally, findings indicate that GBV survivors or those who have witnessed some form of GBV within their immediate families and larger communities are more prone to being targeted online, as corroborated by evidence from Southeast Asian countries of Thailand, Vietnam, and Malaysia (Pradubmook-Sherer and Karansupamas 2020; Nguyen et al. 2020; Marret and Choo 2017):

“Violence in the family, in the school and in the community is related to the higher victimization rates. Being surrounded by violence increases the likelihood of victimization.” –Pradubmook-Sherer and Karansupamas (2020)

Familial power dynamics also play an important role in many contexts across Asia. Policing and surveillance of online activities by family members and kinship networks can often be seen in “honor cultures” where, for instance, brothers position themselves as protectors of their sisters, guarding their mobility and dignity for the sake of family honor. Young women from Southern India report having access to social media or the internet only through a male family member’s device and, in some cases, are compelled to share account credentials with them (Gurumurthy, Vasudevan, and Chami 2019). In the same study, a young woman said that her family encouraged girls to form joint social media accounts with male relatives, usually brothers. Consequently, a woman’s online presence is watched, supervised, and shaped by influence from male family members (Gurumurthy, Vasudevan, and Chami 2019).

Cultural taboos surrounding sex and sexuality are key to understanding technology-facilitated GBV in Asia (Hassan, Unwin, and Gardezi 2018; Akter 2018; Aksar et al. 2020). Participant responses from Hassan et al.’s (2018) study in Pakistan demonstrate one perception that elements of sexual frustration fuel inappropriate sexual behaviors conducted online and offline:

“Most people don’t marry until well into their twenties or thirties, and hence stay virgin for almost half of their lives (statistically). The sexual energy has got to come out somewhere, so it comes out in the form of harassment and cat calling.... It doesn’t happen as often through phones as it does through social media and on the streets.” –Respondent in Hassan, Unwin, and Gardezi (2018)

When public discussion surrounding all aspects of sex is discouraged, this can also prevent productive conversations and understanding of what constitutes healthy sexual dynamics (Nova et al. 2018). A lack of societal understanding of and respect for the concept of consent particularly can play a key role in the perception of technology-facilitated GBV. One source notes in the context of India:

“The idea that a woman can be approached without her consent, and that you can get casual to her, is utterly normalized, and this is what lies at the heart of the worst crimes online.” –Devika et al. (2019)

During one incident in Bangladesh, a female student whose images were distributed without her consent was expelled from her university. She not only faced repercussions for her participation in the initial consensual exchange but was not offered support from the legal system, which believed that because she gave consent to take the photographs she must have given consent for dissemination as well. In the aftermath, one source reflects:

“The notion that consent is not implied for all acts but must be separately sought and taken does not seem to be well understood.” –Chowdhury (2016)
In turn, when such taboos interact with factors of social status and honor, they can feed into a significant fear of “reputation damage” to the “self, family and community” (Sambasivan et al. 2019). If an individual is targeted by online sexual harassment or exploitation, such taboos may act as a barrier for survivors to report their experiences or disclose to their family and friends to seek support. This also fuels perpetrators’ ability to leverage such societal shame for exploitative intentions, as demonstrated by study participants’ experiences in Pakistan and India:

“Our society isn’t open to any relationship between men and women except marital. Those who date or go out, are not considered respectable, and there is a lot of family pressure on young boys and girls to refrain from dating, as a result many go out illegally (according to the socio cultural norms and unacceptability).... Many men then harass or torture their ex-girlfriends using mobile device by sharing their photos, leaking messages.... They use this element as the biggest threat and torture to these women (in case they breakup) knowing that the society will ridicule them and judge them based on their illegal relationship.” –Respondent in Hassan, Unwin, and Gardezi (2018)

“A cyberactivist interviewed for the research in Kerala shared a case where a young teenager was blackmailed and forced by her cousin to have sex with strangers. He threatened to expose her secret outing with college friends by releasing photos that could get her into trouble with her family.” –Gurumurthy, Vasudevan, Chami, and Mahesh (2019)

In the context of patriarchal societies in South Asia, evidence further suggests that conducting such behavior through technology is not only condoned but often appreciated and lauded (Vashistha et al. 2019). For example, regional films in South Asia often normalize inappropriate behaviors in the context of pursuing romantic relationships, such as stalking. In turn, this provides frameworks to perpetrators for non-consensual relations that extend to online behaviors, such as cyberstalking (Sambasivan et al. 2019).

Society also normalizes the idea that online violence cannot have grave impacts on its targets, especially when compared to physical violence (Brazal 2020). For example, a male participant of a study in India expressed during focus group discussions (FGDs) that his male peers do not perceive technology-facilitated GBV as a serious violation:

“While some friends were willing to be reflective, most members in the group shrugged it off, saying, ‘no woman is going to jump from the top of a building just because of a video of her in a bathroom.’” –Devika et al. (2019)

Societal perceptions and patriarchal norms often drive the scrutiny of targets of technology-facilitated GBV rather than condemn the actions of the perpetrator, as reflected by how women and girls are often “blamed” for the violence they face online (Chowdhury 2016; Ramaseshan et al. 2019; Gurumurthy, Vasudevan, Chami, and Mahesh 2019; Dunn 2020; Rallan and Vig 2019; Hassan and Unwin 2017; Wachs et al. 2016). Women are expected to bear the responsibility of controlling online attacks and self-censoring (Brazal 2020). As one source (Kovacs, Padte, and SV 2013) observes:

“There is a perception of women ‘deserving’ abuse for being online, similar to the purposeless presence of women on the street ‘asking for it.”’ –Kovacs, Padte, and SV (2013)
In **India**, for instance, law enforcement expresses more sympathy toward “innocent” women who have been “seduced” and less so toward women who face violence for voicing “strong opinions online and participation in online debates” (Devika et al. 2019). Such perceptions often lead to repeated victimization (Ahmed 2020; Nova et al. 2019), and women who are active and vocal online, particularly in expressing their opinions on gender issues and patriarchy, are especially at risk as they are more likely to experience pushback for defying authority or challenging traditional values (Sarkar and Rajan 2021; Kovacs, Padte, and SV 2013). This is especially seen in occurrences of gendertrolling, a mass-organized act of misogynistic online violence usually perpetrated by male-identifying strangers who come together to intimidate and overwhelm the targeted individual through insults, slurs, and threats of violence (Gurumurthy, Vasudevan, Chami, and Mahesh 2019). In one instance, a woman editor for BuzzFeed in **India** was subject to rape threats and abusive comments from men, including prominent writers, after she tweeted praises for **Pakistan’s** team during an India-Pakistan cricket match (Pasricha 2016).

As a result of deeply ingrained norms—and to potentially avoid being targets of such vicious attacks—some women feel that they must “manage their voice and visibility responsibly” online and avoid “uses that may make one socially vulnerable” (Gurumurthy, Vasudevan, and Chami 2019). Unfortunately, this can escalate into women perpetuating victim-blaming, as one source from **India** notes:

> “Young women are particularly critical of other women whose pictures get leaked online, judging victims of violence for their lack of caution and rectitude, rather than unequivocally condemning the male perpetrator for his acts of violence.” –Gurumurthy, Vasudevan, Chami, and Mahesh (2019)

Continual minimization and normalization of gender-based violence by society is consequently internalized by some women, and they may trivialize their own experience of technology-facilitated GBV. Barriers to reporting and receiving timely and proper support further discourage women from acknowledging the violence and seeking help. One study in **Pakistan** (Digital Rights Foundation 2017) observes:

> “It is nothing new for women to downplay or ignore threats and abuse that they face on a daily basis. Often the only form of abuse, even in the case of stalking, that is acknowledged is when it poses a credible threat of physical violence.” –Digital Rights Foundation (2017)

Denial and minimization can often be coping or processing mechanisms for survivors of trauma and reflect internalized messages received from surroundings (Forde and Duvvury 2021; Sinko et al. 2021). In this context, it highlights that harmful societal factors must be understood not just in their role as drivers of violence perpetration but also in how they can manifest in and add to the enduring impacts experienced by targets of technology-facilitated GBV.

**TECHNOLOGICAL LANDSCAPE**

The increasing anonymity of technology along with its ease of access and wide reach are key factors that facilitate technology-facilitated GBV in Asia. Social media offers a space in which users’ anonymity makes women more vulnerable to male acquaintances, especially those known in family and friend circles, in a way that might deter them from immediately reacting against the abuser in light of kin obligations. Recognizing this advantage of anonymity, male users can exploit women’s vulnerability online (Datta et al. 2020; Devika et al. 2019). Moreover, it is easy for family members and romantic partners to gain access to an individual’s whereabouts or private information to track them (Dunn 2020). From this safe
hidden role, perpetrators commit multiple acts of technology-facilitated GBV without fear of consequences. This allows perpetrators to leave no trail of evidence and create multiple identities—in turn, the victim never knows the perpetrator’s true identity (Fitriana, Souket, and Yie 2020; Leng, Khan, and Rahim 2014). In the case of cyberbullying, unlike traditional bullying where there is face-to-face contact, perpetrators often feel less remorse because they are unable to feel or witness the harm they inflict (Fitriana, Souket, and Yie 2020; Chahal et al. 2019; Sarkar and Rajan 2021).

“Survivors of cyber violence also felt that their perpetrators’ show of such power was due to the absence of physical contact sometimes. This power is amplified because of the ability to maintain anonymity and complicity.” —Sarkar and Rajan (2021)

While there is increased access to technology, at the same time, in some countries of the Asia region there is a growing digital divide in terms of access and usage of technology. The gendered digital divide in some countries of Asia also predisposes women to experiencing technology-facilitated GBV (Cai et al. 2021); women, girls, and marginalized groups with limited digital skills for safe participation online are more at risk of technology-facilitated GBV and are “easy targets” of abuse (UN Women 2020; Cai et al. 2021; Xu 2010).

Lack of accountability on the part of tech companies, limited privacy settings, unclear reporting mechanisms to law enforcement, and unclear consequences for perpetrators are additional factors that promote and prolong experiences of technology-facilitated GBV. For example, the fact that most social networking sites require users to provide identifiable information such as their email address, phone number, and birth date enables perpetrators to easily hack accounts (Ghazali and Ghani 2018). Intimate partners are able to gain access to accounts through social engineering because they know enough to answer security questions or guess passwords (Dunn 2020). Rapidly changing technological landscapes can make timely adaptation or creation of legal frameworks difficult. For example, Halder (2017) notes that non-consensual distribution of intimate images is facilitated by the fact that available laws or frameworks, especially in Bangladesh, India, and Pakistan, do not have any regulations specifically against creation of fake.

CHARACTERISTICS OF PERPETRATORS AND SURVIVORS

Given the anonymous nature of the online space that enables users to conceal and manipulate identities, it is difficult to accurately discern information about perpetrators, such as their gender, age, location, profession, and relationship to their targets. However, the reviewed literature indicates trends in perpetrator profiles across countries in Asia. Additionally, the risk of being targeted by this form of violence seems to vary by an individual’s gender, sexual orientation, caste, religion, nationality, economic status, political affiliation, and profession, among other aspects of their identity.

GENDER

Although both men and women are impacted by technology-facilitated GBV, women and girls in Asia face harassment that is gendered and sexual in nature at disproportionally higher rates compared to men and boys (Xu 2010; Kovacs, Padte, and SV 2013; Gurumurthy, Vasudevan, Chami, and Mahesh 2019). Online perpetration of violent behaviors across Asia is most often conducted by men (Marret and Choo 2017; Mardianto et al. 2019; Devika et al. 2019), although this trend varies depending on the form of technology-facilitated violence. Women in Bangladesh, India, and Pakistan face “multiple,
recurring and interrelated forms of gender-based violence online,” particularly: online harassment, cyberbullying, cybercrimes, and cyberstalking (Akter 2018; Quilt.AI and ICRW 2021; UN Women 2020; Digital Rights Foundation 2017; Kovacs, Padte, and SV 2013; Devika et al. 2019; Amnesty International 2020; Gurumurthy, Vasudevan, Chami, and Mahesh 2019; Nova et al. 2018; Hassan, Unwin, and Gardezi 2018; Adebayo, Ninggal, and Bolu-Steve 2020; Halder 2017; Chahal et al. 2019; Randhawa 2010). During the COVID-19 pandemic, more women have been active in cyberspace, which has further heightened their risks of experiencing online violence (UN Women 2020; Cai et al. 2021).

Study findings show that men and boys are both perpetrators and targets of cyberbullying. For instance, in Malaysia, Adebayo et al. (2020) found that among high school and undergraduate students, boys and young men are the primary perpetrators of cyberbullying, and Fitriana et al. (2020) found that Malaysian men are also more likely to be victims of traditional bullying and cyberbullying (Adebayo, Ninggal, and Bolu-Steve 2020; Fitriana, Souket, and Yie 2020). In Pakistan, the evidence is more consistent that men are more likely than women to bully women online (Musharraf et al. 2019; Khawar and Malik 2016; Hassan and Unwin 2017). This is in part attributed to the fact that in Pakistan, boys usually have easier access and more exposure to technology and electronic devices, compared to girls who are more carefully monitored by parents (Khawar and Malik 2016).

However, as noted by Balakrishnan et al. (2015), the gendered aspect of cyberbullying is difficult to determine because both genders appear to be equally affected. This is in line with findings from India, where young men are often bullied by fellow young men for promoting feminist and gender non-conforming views, as it is seen as a deviation from otherwise socially defined gender norms (Devika et al. 2019). The following excerpt captures this finding:

“Given this normalized toxic macho culture circulating among young men, it is no surprise at all that in almost all the high-profile mass cyber-bullying cases, the culprits nabbed have tended to be young men, often teenagers. Breaking with such groups or dissenting within carry huge consequences, as noted by a male student who identified as a feminist. His positions against normalized misogyny in young male groups made him a target of intense attacks. The attacks against dissenting men too can be highly gendered.” –Devika et al. (2019)

Unlike the case with cyberbullying, there is growing evidence indicating that cyberstalking is usually perpetrated by males against females and stems from male entitlement (Dunn 2020; Gurumurthy, Vasudevan, and Chami 2019). In a 2019 study from India, researchers found that in more than 70 percent of cases, women were cyberstalked by men (Chahal et al. 2019). Similarly, in Pakistan, as men continue to retain control over technology, mobile phones are commonly used to harass and stalk women, either from anonymous callers or as part of an ongoing abusive situation (Randhawa 2010).

As mentioned previously, non-consensual distribution of intimate images is a highly gendered phenomenon often perpetrated by men, who request intimate information and photos after gaining the trust of their partner (Dunn 2020). For example, a common pattern in Bangladesh finds male perpetrators having physical relationships with their partners in supposedly safe spaces (e.g., hotel rooms or a friend's house), only for the perpetrator to later threaten the distribution of photos or videos captured through hidden cameras (Akter 2018; Gurumurthy, Vasudevan, Chami, and Mahesh 2019).
With regard to cybergrooming, perpetrators are predominantly older males, although there is some evidence that women also use technology to groom adolescents, especially male victims (Wachs et al. 2016). Findings from Thailand indicate that in cases of online sexual solicitation and cybergrooming, the perpetrator is usually of the opposite sex—meaning males are solicited by females and vice versa. However, it is possible that gender reporting for this form of violence could be biased, as male targets may experience shame associated with being groomed by perpetrators of the same sex and therefore report instead that the perpetrator was female (Wachs et al. 2016).

LGBTQI+ persons face high rates of online harassment in several countries of the Asia region, including India, Indonesia, and Bangladesh, on the basis of their sexual orientation (QUILT.AI and ICRW 2021; Dunn 2020; Wahyuni, and Baadila 2015; Gurumurthy, Vasudevan, Chami, and Mahesh 2019). They are especially vulnerable when information is made available online without their consent, risking exposure of their gender and sexual identities (Chowdhury 2016). Findings from India indicate that not only are transgender women more at risk of experiencing online harassment compared to cisgender women, but people writing about LGBTQI+ issues also experience online harassment (Pasricha 2016; Devika et al. 2019). In Pakistan, individuals identifying as gender non-binary have faced increased cyber harassment during the COVID-19 pandemic (Digital Rights Foundation 2020). Another study reveals that gender minorities along with intersecting marginalization (individuals who are younger, low-income, rural, with disabilities) have reported to be more vulnerable than other individuals to experience abuse online in India, Pakistan, and Bangladesh (Sambasivan et al. 2019). Moreover, in such countries where LGBTQI+ issues are condemned by the government, abuse perpetrated online tends to be homophobic and misogynist (Posetti et al. 2021).

**AGE**

Age-specific differentiation in the experience of technology-facilitated GBV and online victimization varied across countries in the Asia region. Age-disaggregated data are mostly available for cases of cyberbullying; few studies provide gender-disaggregated data, instead referring to age cohorts like students, youth, and adolescents. However, one study from Pakistan showed no significant difference found in cyberbullying victimization in relation to age (Saleem, Khan, and Zafar 2021).

Several studies reinforce women’s vulnerabilities related to age and being subjected to violence online. In India, women ages 16–35 years are vulnerable to online cyber scams or frauds (Datta et al. 2020), and adult women are often survivors of NCII in India, Bangladesh, and Pakistan (Halder 2017). Similarly, in Nepal, young female journalists ages 21–25 years have experienced more sexual and non-sexual insults and threats online, compared to female journalists older than 35 years (Koirala 2020). Pakistani women ages 18–25 years are most vulnerable to threats related to physical abuse, cyberstalking, receiving inappropriate pictures and unwanted messages against their will, and online harassment (Digital Rights Foundation, 2017).

Furthermore, both women and men have experienced cyberbullying in Myanmar by age 20 or younger (Khine et al. 2020), and in Thailand, male students ages 14–17 years are more vulnerable to cyber victimization than older students (Pradubmook-Sherer and Karansupamas 2020). In Malaysia, children and teenagers ages 5–18 years are most vulnerable to online harassment (Ghazali and Ghani 2018). The same is true in India and Pakistan where youth are more vulnerable to online harassment and cyberbullying than older social media users (Wachs et al. 2016; Musharraf and Anis-ul-Haque 2018; Bhat et al. 2017; Jain and Agrawal 2020).
Instances of hacking and identity theft are common among young users in **Malaysia** (Ghazali and Ghani 2018). In cases of cybergrooming, the majority of respondents from a 2016 study indicated that they were not aware of the perpetrator’s age and those who were aware of this information indicated that the cybergroomer was often older (Wachs et al. 2016). This trend is consistent with findings from **Bangladesh** where adults “groom” or build trusting relationships with children since they are able to conceal their true age, giving the child a sense of false security (Chowdhury 2016). Given more consistent access to the internet and social media, university students are more likely to engage in cyber aggression than those in high school, as the latter group has more limited and monitored access to technology (Chowdhury 2016). With respect to cyberbullying, Bhat et al. (2017) found that in **India**, the risk of being a cyberbully is higher among youth ages 13–17 years than those aged 8–12 years. Mardianto et al. (2020) found that in **Indonesia**, excessive use of ICTs has the potential for internet abuse among adolescents and often leads to cyber aggression, especially among those who are emotionally vulnerable and easily triggered.

**MARGINALIZED AND VULNERABLE GROUPS**

Technology-facilitated GBV in the Asia region has adversely impacted marginalized and vulnerable people, especially those who are women and girls. As seen in **India**, women with intersecting marginalities, such as lower caste status (e.g., Dalit), religious minority (e.g., Muslim), non-heteronormative gender identities, low socioeconomic status, and older age group, were most at risk of experiencing online harassment and abuse—thus, amplifying their marginalized status (Gurumurthy 2019; Munusamy 2018; Xu 2010; Gurumurthy, Vasudevan, and Chami 2019; QUILT.AI and ICRW 2021). One study noted, “Women from marginalized castes received 59 percent more casteist slurs than women from general castes” and that “Muslim women receive more religious and ethnic slurs and racism-based abuse than Hindu women in India” (Amnesty International 2020). Another study (Gurumurthy, Vasudevan, Chami, and Mahesh 2019) stated:

> “Dalit women encounter caste-based violence along with sexual violence online…. The abuse often takes the shape of criticism of choices (especially consumption of meat) to deride caste based cultures. When being trolled, as with the case of a survivor we interviewed, pictures of the woman eating meat may be pulled up to allege religious betrayal and drum up anti-national claims.” —Gurumurthy, Vasudevan, Chami, and Mahesh (2019)

Similarly, in **Pakistan**, individuals belonging to ethnic and indigenous minorities are more vulnerable to online violence (Digital Rights Foundation 2020). Globally, female politicians and journalists have become a target of online abuse and harassment (Gurumurthy, Vasudevan, Chami, and Mahesh 2019; Di Meco 2019; Mukherjee, Ratho, and Jain 2021; Amnesty International 2020). In **India**, secular journalists and women’s rights activists are increasingly being subjected to online harassment threats and gendertrolling (Gurumurthy, Vasudevan, Chami, and Mahesh 2019; Pasricha 2016). Similarly, **Filipino** women activists and journalists who question government policies are subjected to sexual harassment online (Brazal 2020; Chahal et al. 2019):

> “It is also notable that journalists across our sample shared many similar experiences, despite different cultures and media systems. Consistently, the journalists we interviewed saw online gendered harassment as hampering their efforts to report the news, engage with the communities they cover, or have a voice in the digital sphere. An Indian online editor explained—Sex is used to intimidate us. Rape is used to frighten, intimidate, and stop us … from doing our work, but at a deeper level it is
actually about stopping us from having opinions, showing any semblance of independence.” –Chahal (2019)

Some studies have shown that, as seen in the Indian context, cyber harassment can be based on women’s physical appearance and their intersecting social identities (Gurumurthy, Vasudevan, Chami, and Mahesh 2019; Rafi 2019; Munusamy 2018; Gurumurthy, Vasudevan, and Chami 2019; Dunn 2020). The following quote summarizes this vulnerability:

“This moral policing of dress code happens much more to dark, fat women rather than those who are fair and thin. This is only a simple demonstration and there is a flood of casteist, racist, sexist, extremist, hateful and chilling contents on social media” –Munusamy (2018)

Furthermore, in India, individuals coming from privileged backgrounds, including upper caste Brahmins and especially men, receive significant protection even when their intention is to harass, abuse, defame, and threaten (Munusamy 2018).

RELATIONSHIP TO PERPETRATORS

In Asia, many instances of technology-facilitated GBV are committed by strangers. In a recent study, respondents from India noted receiving unsolicited messages from strangers on social media:

“During the initial stages when I joined Facebook, I used to receive a lot of messages from people I didn’t know. The language and content of those messages were not appropriate, and they made me feel angry and afraid and uncomfortable. The guy was a stranger online and after I just asked him how do you know me, he sent the picture of his dick, trying to be proud of his senseless action.” –Gurumurthy, Vasudevan, Chami, and Mahesh (2019)

Cyberstalking is a highly anonymous crime, and data suggests that perpetrators of cyberstalking are most likely to be strangers to or acquaintances of survivors, such as taxi drivers or delivery agents. In some cases, men also pose as women for the purpose of gaining trust of the women they are harassing and to access their information with greater ease (Sambasivan et al. 2019). Perpetrators have also been known to create fake profiles to carry out cyberstalking and eventually threaten targets and their families with dissemination of explicit materials (Halder 2017)

In Bangladesh, it is common for girls to accept online friend requests from strangers, who may begin blackmailing them after a friendship or relationship develops between the two individuals through online communication. Another example is of couples being filmed by strangers without their knowledge through hidden cameras in hotel rooms. However, as noted in the following excerpt, it is also found that sometimes women are harassed by known individuals using a different name online (Sultana et al. 2021; Chowdhury 2016; Bhattacharjya et al. 2011):

“Himani was harassed online by a ‘stranger’ who she later found out was a senior at school whose friendship requests she had repeatedly ignored.” –Bhattacharjya et al. (2011)

Moreover, there is also some correlation between the openness of the platform and the prevalence of perpetration by anonymous users. For instance, analysis of survey results indicates that social networking sites such as Facebook and Instagram have a high proportion of unknown perpetrators because they are designed to be open access, whereas WhatsApp has more known perpetrators
because it typically used to communicate with people who have each other’s number and have had prior contact offline (Gurumurthy, Vasudevan, Chami, and Mahesh 2019).

Another study found that among Indian youth, a quarter of their Facebook friends are people whom they have never met and will likely never meet. Friendship decisions are based on profile photos and the nature of their posts and are seen as a pathway for more romantic inclinations, suggesting that youth exercise less reservation toward strangers and are more likely to accept friend requests from strangers who are often perpetrators of online abuse (Arora and Scheiber 2017).

Although in many cases, technology-facilitated GBV is perpetrated by strangers, acts of online violence are also committed by known individuals. Only a few studies reported on technology-facilitated GBV committed by work colleagues and supervisors. A study from Nepal found that although the majority of online abusers were anonymous or unknown individuals, 15 percent of respondents experienced online harassment by their male colleagues or supervisor (Koirala 2020). Similarly, the following excerpts from separate studies in India (Gurumurthy, Vasudevan, and Chami 2019; Bhattacharjya et al. 2011) recount how individuals can be doxed or outed by their colleagues, which can severely impact their professional lives:

“Jealous male colleagues had targeted the two women, creating fake profiles of them on matrimonial sites and linking this to their official email IDs. As a result of this, the women were flooded with unwanted emails. This had severe repercussions on their work.” –Gurumurthy, Vasudevan, Chami, and Mahesh (2019)

“I was relatively new to the internet so I think I downloaded a virus from there by mistake. To take out this virus all our personal stuff was checked and seen by the office IT people and it quickly spread round that I had looked at these queer sites and I was hauled up for it by the editor for using the internet for “personal gain”, [and she] also revealed to everyone that I was looking at gay sites. That’s how she outed me. It was devastating. It was terribly humiliating because I had no choice in deciding to let everyone in the office know that I am gay…. I ended up getting fired from this job and it took me a long time to recover.” –Bhattacharjya et al. (2011)

IMPACTS OF TECHNOLOGY-FACILITATED GBV ON SURVIVORS

The research team found that many peer-reviewed and grey literature articles dedicate attention to the wide-ranging impacts that survivors experience during and after an incidence of technology-facilitated GBV. Some impacts were minor, while others were described as more serious and long-lasting.

“It seems beyond question to us that GBCV [gender-based cyber violence] is indeed widespread and it causes serious, if often, unnoticed, harm to young women, results in loss of mobility, confidence, social standing, and voice; it can lead to curtailment of ongoing education and work as well as loss of future opportunities; it can lead to physical punishment of these women offline and also to their bodily harm and loss of health. In other words, the widespread idea that GBCV, especially that suffered by vocal women online, is trivial and easily eradicable through exiting the internet is simply wrong.” –Devika et al. (2019)

In this section, these impacts are discussed based on the ICRW framework (Hinson et al. 2018), grouped as follows: physical, psychological, social, economic, functional, and aspirational.
PHYSICAL IMPACTS

The physical impacts on survivors include everything from health issues to murder and suicide.

A study from the Philippines on online child sexual abuse reports individual symptoms, including abdominal pain, cardiovascular problems, and metabolic disorders (Merten 2020). Devika et al. (2019) describes psychosomatic ailments among those who had been cyber-harassed in India. Several articles mention drug use as a coping mechanism (Ghazali and Ghani 2018; Brazal 2020; Fitriana, Souket, and Yie 2020; Akter 2018), while self-harm is mentioned in the context of cyberbullying (Nguyen, Nakamura, and Vo 2020). Suicide and suicidal attempts are mentioned in a few articles (Akter 2018; Ghazali and Ghani 2018).

“From 2010 to 2014, Bangladesh National Woman Lawyers’ Association identified a total of 65 reported suicide attempts by female victims of violence. It also reveals that on an average, every year there are 11 suicide attempts by women due to cyber violence.” –Akter (2018)

In terms of harm caused by others, both strangers and families are implicated in committing some of the more serious physical impacts, including acid attacks and rape. In extreme cases, victims are murdered; for example, the infamous 2012 Pakistani Kohistan honor killing case in which several girls were murdered by male family members after a video emerged online featuring them clapping and singing along while a boy danced during a wedding celebration (Hassan, Unwin, and Gardezi 2018).

PSYCHOLOGICAL IMPACTS

Psychological impacts are commonly documented in the literature and include feelings of fear, depression, isolation, anger, guilt, helplessness, embarrassment, self-blame, and apprehension. For example, survivors of online child sexual abuse in the Philippines describe a loss of confidence and low self-esteem (Merten 2020). Several articles describe survivors as experiencing post-traumatic stress syndrome or other severe psychological injury, including withdrawal (Ramaseshan et al. 2019; Abbasi et al. 2019; Sambasivan et al. 2019).

“Research studies on the effects of non-consensual circulation of intimate images – often referred to as ‘revenge porn’—usually by an ex-partner, as an act of revenge, have found that survivors feel suicidal tendencies and feelings of depression and anxiety and sometimes, even, post-traumatic stress disorder. Loss of control, lack of confidence, and decreased self-esteem may also result.” –Gurumurthy, Vasudevan, Chami, and Mahesh (2019)

It is common for threats of and consequences from physical and sexual violence to target not only survivors, but also their families and communities. Families may experience social isolation, exclusion, humiliation, and public resentment due to the experience of one family member. In many cases, the impact (or the potential for this kind of impact) is more disturbing to the survivor than the personalized threats they receive (Akter 2018; Koirala 2020).

SOCIAL IMPACTS

The social impacts of survivorship are myriad, leaving individuals and their families in complex situations. Impact is deeply felt when the violence experienced was sexual in nature, such as the sharing of non-consensual material (Posetti et al. 2021; Ramaseshan et al. 2019):
“Participants [in Bangladesh, India, and Pakistan] described how reputation damage was rooted in the suspicion of a woman’s presumed complicity and looseness in leaking sexual content about themselves, even when the release was non-consensual (due to presumed sexual and pre-marital relations, considered taboo for most women).” –Sambasivan et al. (2019)

Survivors in Bangladesh, India, and Pakistan face threats and abuse from friends, as well as discrimination and coercive sexual threats from strangers (Sambasivan et al. 2019). Other social impacts in India include individuals’ loss of freedom to move about without adult permissions and the expulsion from social activities (Devika et al. 2019). Authors of a study in Bangladesh report that social ramifications extended to the family, who also experienced social exclusion, humiliation, and public resentment (Akter 2018).

Girls’ online expression and voice are curtailed and censored; oftentimes, the family members of the girls who experienced online abuse are the ones restricting these social freedoms (Posetti et al. 2021). In fact, the loss of freedom of expression for survivors of technology-facilitated GBV, especially for girls and women, arises in several sources (Mukherjee, Ratho, and Jain 2021; Chowdhury 2016; Sarkar and Rajan 2021):

“Out of the 30 participants, 20 of them have withdrawn from the public sphere because of fear of their family’s safety, perpetrator’s anonymity and complicity of what they are experiencing.” –Sarkar and Ranjan (2021)

Social impacts of technology-facilitated GBV extend to the marriage and relationship context, including being forced to marry someone (Hassan and Unwin 2017), losing marriage opportunities, or having to submit to coercive romantic relationships (Sambasivan et al. 2019, (Hassan, Unwin, and Gardezi 2018).

“Others commented that many parents would force their daughter to marry another man of their choosing if they became aware through imagery or text on social media that she had had any kind of relationship with someone…” –Hassan, Unwin, and Gardezi (2018)

ECONOMIC, FUNCTIONAL, AND ASPIRATIONAL IMPACTS

Several articles discuss the economic, functional, and aspirational damages caused by experiencing technology-facilitated GBV.

Economic impacts include threats or real disruptions to one’s livelihood. Two sources from India describe scenarios in which participants experienced economic impacts. One survivor described being expelled from his family and forced to support himself financially (Devika et al. 2019). Another source reported that some participants were blackmailed (for money or personal information) or received messages blackmailing them into sex on the threat of leaking their intimate pictures online (Gurumurthy, Vasudevan, and Chami 2019; Posetti et al. 2021).

Functional impacts refer to various experiences that disrupt the daily routines in one’s life. One Sri Lankan woman was forced to move and eventually flee the country with her family (Posetti et al. 2021). Children in the Philippines who were sexually abused online were also less likely to go to school and experienced educational delays (Merten 2020). Other sources described a disruption of education and opportunity, absenteeism at work, and being fired from jobs (Devika et al. 2019; Akter 2018; Ghazali and Ghani 2018).
Several sources report aspirational impacts, referring to the curtailing of occupational and educational goals and desires (Devika et al. 2018; Koirala 2020). For example, one source from Nepal notes that survivors in certain career paths, such as journalism, decided to leave their career entirely after their experiences (Koirala 2020):

“Because of the repeated incidents of similar harassment, she stated that she was considering changing careers shortly. She said: I received several messages on my Facebook and Twitter, most of them in the form of private messages. It included physical threats and some of the comments were also sexist in nature…. I am so frustrated that I want to leave this profession. (Interviewee, July 22, 2019)” –Koirala (2020)

HELP-SEEKING BEHAVIORS OF SURVIVORS

Help-seeking behaviors are the actions, or lack thereof, that survivors take as a result of experiencing technology-facilitated GBV. These actions include reporting incidents to the authorities or the platforms on which they were experienced; seeking support from professional sources, family, friends, peers, or online platforms; modifying online behaviors; or avoiding taking any action at all. These actions or non-actions are directly linked to the response and prevention tactics used by various actors that play a role in addressing technology-facilitated GBV, including family, friends and peers, technology companies, schools, workplaces, and the government. Understanding the challenges survivors face when trying to seek help after an experience of violence and what forces enable or deter them from accessing a successful response is important for future programmatic and policy efforts.

The research team organized results by the various stakeholders and systems (e.g., technology companies, government and law enforcement, workplace, schools, and the larger community) that play a role in facilitating or hindering those help-seeking behaviors.

TECHNOLOGY COMPANIES

Most social media, networking, and online dating platforms have methods in place for users to report and flag online harassment, abusive content, privacy violations, and fake profiles. However, many articles found that survivors are overall dissatisfied with the response and prevention tactics of platforms. Sources also mention how underreported crimes are due to the numerous challenges faced when trying to report experiences. Common barriers to reporting on platforms included poor awareness of reporting mechanisms (Devika et al. 2019); perceptions that the platforms would not do anything (Pasricha 2016); and a perception that filing a report is cumbersome and complex (Buhkari 2014).

The most frequent complaint from survivors is that their reports are often ignored, or they are told that the nature of the incident did not violate community standards (Chowdhury 2016; Devika et al. 2019; Ramaseshan et al. 2019). Often platforms use a combination of manual and algorithm-based moderation tactics to review content based on community standards and guidelines (Gurumurthy, Vasudevan, Chami, and Mahesh 2019). This method, and the frequent use of intermediaries to enforce community standards, produces suboptimal results that are vulnerable to vast subjectivity (Gurumurthy, Chami, and Vasudevan 2017). When responses are provided, response times vary based on the platform and the nature of the complaint, with GBV not seen by survivors as a priority for the platforms (Devika et al. 2019; Ramaseshan et al. 2019). Research indicates that platforms are likely to respond to reports of violations unrelated to harassment more quickly, such as copyright infringement (Chowdhury 2016).
Another concern is that the platforms have a “Western bias” in how they review complaints and that they do not see certain things as offensive or do not agree that the complaints violate community standards, and thus nothing is done (Sambasivan et al. 2019; Munusamy 2018; Gurumurthy, Vasudevan, and Chami 2019). For example, in India, respondents discussed how platforms often did not respond to reports when the harassment was harmful slang specific to their culture because they were not able to identify it as violence (Pasricha 2016). Platforms also are usually not transparent about their community standards, making them difficult or impossible to access (Gurumurthy, Vasudevan, Chami, and Mahesh 2019). When standards are published, they are reported almost exclusively in English, creating a further barrier for survivors in trying to report, as they are unable to discern what went against platforms’ community standards. Some platforms’ reporting mechanisms are also only in English, further discouraging survivors to report (Chowdhury 2016; Gurumurthy, Vasudevan, and Chami 2019; Quilt.AI and ICRW 2021; Posetti et al. 2021). Some survivors in India even report a lack of response from platforms when they made complaints in languages other than English (Gurumurthy, Vasudevan, and Chami 2019).

Research also shows that platforms have tendencies to ignore violence when it is in their best business interest. In 2019, the Internet Democracy Project found that websites like PornHub.com and xVideos.com have been accused of delaying the removal of non-consensual content and image-based abuse when they are profiting from the content (Dunn 2020). Facebook has also been accused of putting business and market interest above implementing community standards on gender-based hate speech (Gurumurthy, Vasudevan, and Chami 2019).

“Quantified appreciation through ‘likes’ feedback on what the ‘public’ loves and nudges them to produce more such content. Algorithms order content by popularity, reinforcing market considerations in content production… Reddit’s system of up-voting and down-voting content to earn ‘karma’ points and the ordering of content as per popularity led to a viral spread on the platform of leaked intimate images of female celebrities.” – Gurumurthy, Vasudevan, Chami, and Mahesh (2019)

Some platforms are taking steps toward prevention of online GBV. For example, in India, Tinder piloted a feature that allows only women to message matches first in hopes of decreasing the incidence of harassment for women (Ramaseshan et al. 2019). An Amnesty International report found that in 2019, Twitter took positive steps toward protecting women and girls from online abuse and harassment through enhanced reporting features and user education about online safety (Amnesty International 2020). However, even with these steps toward prevention, research finds that women on all platforms still experience high rates of online violence.

It is important for technology companies to create holistic, intersectional response and prevention mechanisms that effectively and efficiently support survivors of online abuse and harassment and ensure their platforms are safe places to exist online (Posetti et al. 2021; Nova et al. 2019; Di Meco 2019). Security and reporting features should be easy and accessible (Posetti et al. 2021), in local languages, and sensitive to cultural context (Gurumurthy, Vasudevan, and Chami 2019; Buhkari 2014; Chowdhury 2016). Reporting mechanisms should also provide the ability to escalate claims of harassment to take more immediate action against serious and repeat offenders (Posetti et al. 2021; Pasricha 2016). Response and prevention policies and procedures should be reviewed frequently to remain relevant to the constantly changing nature of online activity (Gurumurthy, Vasudevan, and Chami 2019). Overall,
women want to see technology companies taking more responsibility for keeping them safe online through their response mechanisms and prevention tools.

GOVERNMENT AND LEGAL SYSTEMS

Local law enforcement and government authorities have instituted both policy and programmatic responses to address cyber violence to varying levels of effectiveness. Existing laws targeting cybercrimes in the regions studied have increased in recent decades, with most countries having some form of legislation addressing this growing phenomenon. Greater cooperation efforts are also emerging across Asia to tackle online sexual abuse and exploitation of children, with at least seven coalitions, alliances, and taskforces consisting of government, non-governmental organizations (NGOs), companies, and law enforcement (Singh 2018).

However, governments face many response and prevention challenges as they struggle to create cohesive laws and timely policies that capture the increasing avenues of technology-facilitated GBV. Definitions for the forms of technology-facilitated GBV in multiple countries are disjointed, outdated, or non-existent in the laws (Akter 2015; Chowdhury 2016; Halder 2017; Randhawa 2010). Certain cybercrimes can be prosecuted under existing laws, yet the constant growth of the internet has created new forms of violence, such as gendertrolling and doxing, that have no legal precedent and may not be reflected in the law at all (Gurumurthy, Vasudevan, Chami, and Mahesh 2019; Chowdhury 2016; Halder 2017). Though India’s Information Technology Act 2000 has certain provisions on technology-facilitated GBV, such as online rape threats and image-based abuse, the act itself is not specific to cyberviolence against women (Pawar and Sakure 2019). The lack of cohesive legislation leads to a cumbersome system that may confuse lawyers and law enforcement (Gurumurthy, Vasudevan, Chami, and Mahesh 2019; Pasricha 2016).

Law enforcement officers often rely on or default to existing legislation in technology-facilitated GBV cases that may further perpetuate patriarchal norms and discrimination. For example, multiple countries have anti-obscenity or anti-pornography laws that are intended to protect “social morality” rather than the survivor (Gurumurthy et al. 2019; Halder 2017). Laws revolving around public decency increase harm for marginalized communities, such as LGBTQI+ individuals, by labeling sexual expression online as deviant (Boellstorff 2020; Gurumurthy, Vasudevan, Chami, and Mahesh 2019; Xu 2010).

“Despite availability of other progressive legal provisions criminalizing cybercrimes against women, the archaic anti-obscenity sections, both in the [Indian] IPC and the IT Act, continue to be used disproportionately by the police.” –Gurumurthy, Vasudevan, Chami, and Mahesh (2019)

When it comes to enforcing these laws, major bureaucratic, institutional, and cultural barriers within law enforcement and the legal system impede survivors seeking support. One of the greatest reported challenges to filing a formal complaint is the fear that law enforcement is abusive and disrespects women (Sambasivan et al. 2019). Police are known to blame women for their experience during the reporting of a violent event (Kovacs, Padte, and SV 2013; Gurumurthy, Vasudevan, and Chami 2019). Overall, there is a lack of trust in the legal system and law enforcement to take claims of violence seriously and adequately respond. In India, researchers report a lack of trust in institutions to take the crime seriously (Gurumurthy, Vasudevan, and Chami 2019) and a “fear of one’s personal life being made public and the process being humiliating” (Ramaseshan et al. 2019, p.16). One study in Pakistan discusses a
lack of trust leading to a lack of reporting to police, teachers, and community leaders to deal with the issue (Hassan 2018). Some of these fears were born out in real life:

“In Karnataka [India], a survivor interviewed for the research reported how when she took complaints of gender trolling to the police, she was met with a thinly-veiled ‘you were asking for it’ jibe: The police told me, ‘If you don’t provoke them, they won’t say things like this.’ And, this in spite of threats I was getting of rape, acid attack etc.” –Gurumurthy, Vasudevan, Chami, and Mahesh (2019)

In India there is a notion that law enforcement will only take complaints seriously if they result in physical harm (Gurumurthy, Vasudevan, Chami, and Mahesh 2019). Since the harm of technology-facilitated GBV is more often psychological, this leads to an inability of society and survivors themselves to conceptualize the seriousness of the event or categorize the event as “violent” (Pasricha 2016), instead trending toward normalization and trivialization. This prevents many from recognizing and reporting on experiences of technology-facilitated GBV (Sarkar and Rajan 2021; Saha and Srivastava 2014; Digital Rights Foundation 2017; Gurumurthy, Vasudevan, and Chami 2019).

“Women in their narratives called cyber violence an invisible form of violence because most of them when seeking support for it did not know how to conceptualize the seriousness of it.” –Sarkar and Rajan (2021)

Survivors also lack awareness and familiarity with reporting mechanisms, which is another challenge. Many do not even realize reporting is an option (Aksar et al. 2020). People are not aware of the cyber laws that exist to protect them (Aksar et al. 2020; Chowdhury 2016), and many are disinterested or technology-naïve (Kovacs, Padte, and SV 2013). When survivors are aware of their reporting options and do choose to report, they describe finding the process “harrowing and bureaucratic,” with legal agencies outdated in their knowledge of technology (Kovacs, Padte, and SV 2013). Cases of technology-facilitated GBV are overall highly underreported, and few cases that are reported are processed. Survivors sometimes are unable to file the complaint formally without tangible proof of the harassment. For example, in India, cyber sexual harassment cases are usually not processed because it is too difficult to find the culprits (Halder 2017). Some motivators do increase formal reporting among women who experienced harassment: a desire for a sense of justice, preventing violence from happening to others, and exposing the harasser to the public (Sultana et al. 2021; Hassan, Unwin, and Gardezi 2018). One article found that 64 percent of participants believed a woman harassed should inform the police regarding threats to her life both online and offline (Ramaseshan et al. 2019).

The legal barriers that impede reporting show the need for investments in training police forces or creating units to specialize in online violence, which has been a significant government response in some countries (Sambasivan et al. 2019). For example, in India, the national government created the Cybercrime Prevention Against Women and Girls Scheme, which aims to train 27,500 stakeholders across the criminal justice system, including police, prosecutors, and judicial officers in awareness of cyberviolence. It further aims to train 13,500 officials on investigation of cybercrimes and increase the training of women officers specializing in such crimes (Gurumurthy, Vasudevan, Chami, and Mahesh 2019). Bangladesh police have also created a specific “cyber wing” to monitor online crime, though this does not specifically address gender-based online violence (Akter 2018).

Public educational and awareness programming to address the lack of awareness about response mechanisms and harmful cultural norms that perpetuate violence has been a core government response
to technology-facilitated GBV in some countries. Research supports increasing awareness campaigns for adults and children to improve understanding of what online violence consists of and what resources are available to assist survivors (Bhat et al. 2017; Hassan, Unwin, and Gardezi 2018; Sambasivan et al. 2019). Online safety education programs for children have launched in Malaysia and the Philippines (Marret and Choo 2017; Gill 2021). Increased awareness for adults has emerged in the form of online hubs and hotlines for reporting technology-facilitated GBV or learning more about the resources and laws available to assist survivors (Akter 2018; O. Jain et al. 2020).

WORKPLACE AND EDUCATION SYSTEMS

Research finds community settings like schools and workplaces lack support mechanisms for survivors and are underutilized in response and prevention against technology-facilitated GBV. In academic institutions, which are identified as important resources particularly for young people, educators lack the knowledge and curriculum to teach about online safety and cyberbullying prevention (Gurumurthy, Vasudevan, and Chami 2019). Research from Vietnam, India, and Thailand all report that educators lack the necessary awareness to teach about the risks of being online, and school curriculums often do not include cyberbullying in their traditional bullying programming (Sittichai 2014; Le et al. 2016; Bhat et al. 2017). This ultimately creates knowledge gaps for students, leaving them vulnerable to both cyberbullying and cybervictimization.

Even when reporting and prevention mechanisms are in place, students lack awareness of their options or trust that their school would act (Gurumurthy, Vasudevan, Chami, and Mahesh 2019; Gurumurthy, Vasudevan, and Chami 2019). For example, a law in India mandates that universities must have an internal committee on sexual harassment, which includes handling complaints about online sexual violence. However, awareness of these kinds of committees is low among students (Gurumurthy, Vasudevan, Chami, and Mahesh 2019; Gurumurthy, Vasudevan, and Chami 2019). Among those who are aware of their existence, students lack trust that their reports of online sexual violence would be met with sensitive and appropriate responses rather than victim-blaming (Gurumurthy, Vasudevan, and Chami 2019; Ramaseshan et al. 2019). Students also feel school officials are not educated enough about online victimization to help them address it, a sentiment that transcends all levels of educational institutions.

“Schools and parents are uncomfortable broaching the topics of sexuality and online harm, and uncomfortable using technology, therefore leaving a gap in education for young people” –Bhattacharjya et al. (2011)

Workplaces such as news organizations and media outlets also do not have proper response and prevention mechanisms in place to protect their employees from online violence, especially women journalists (Chen et al. 2020). Overall, women journalists report having high expectations to engage online with little to no support from management when they experience harassment, reporting that management staff often seems disconnected from the experience of online discourse (Chen et al. 2020). Women employees, especially, report not being offered any kind of support from their employers, including training on how to deal with harassment or stay safe online, policies for reporting practices, or actionable employer response plans, such as scripts for women to use to ward off harassers (Chen et al. 2020). Employees have little confidence in their employers to hear their complaints or act on their behalf if they report experiencing online abuse (Chen et al. 2020). Women in male-dominated, public-facing careers like journalism have come to expect online violence (Kumar, Gruzd, and Mai 2021).
“We are encouraged to go online to promote our stories on Twitter and Facebook, but there is little training given to us. We aren’t taught about how we can stay safe online … how to interact with comments online … how to deal with trolls…. Organizations expect us to use online resources for promotions but won’t take any responsibility for any backlash we may face” –Chen (2020)

Community settings like schools and workplaces have been identified as important areas to institute programming for addressing technology-facilitated GBV. In order to address knowledge gaps faced by adolescents, schools should be implementing curriculum for students to understand the broader risks of being online, safe ICT use, respect for others, privacy and consent, and empowerment approaches for both boys and girls. Schools should also be training educators to adequately teach their students this curriculum (Wachs et al. 2016; Fitriana, Souket, and Yie 2020; Rallan and Vig 2019; Wright et al. 2016). Workplaces are also areas for increased awareness and education programming. Employees, especially women, want training for all staff on the hazards of engaging online, scripts for warding off harassment, and lessons for employees on how to ensure their safety and report incidences of violence (Chen 2020).

SOCIAL SUPPORT SYSTEMS

Only one article mentions survivors seeking help from professional counselors or experts when experiencing technology-facilitated GBV (Adebayo, Ninggal, and Bolu-Steve 2020). Instead, when they choose to seek support, survivors more often turn to social support systems of family, friends, or peers. Family support is found to be an important factor in enabling women and adolescents to seek response for online harassment (Devika et al. 2019; Sambasivan et al. 2019). However, effective family support is contingent upon how well equipped the family is to address the needs of the survivor, and research shows that parents and other family members are often ill equipped to effectively prevent and respond to online violence. Most survivors choose not to share their experience of online harassment with family members, citing lack of empathy and understanding, disinterest, lack of knowledge about technology, not having close relationships with their family, and fear of being cut off from online activities. Survivors also perceive that parents and family members are likely to blame them for their experiences or not believe them (Devika et al. 2019).

“The importance of continuing to remain online is testified by the reluctance of victims to seek help from family for fear of their access being cut off. 54 percent of respondents who had faced cyberviolence reported that they would not seek help from parents or relatives. Nearly half of this number reported that this was because they were worried their mobile phone/laptop/gadget may be confiscated.” –Gurumurthy, Vasudevan, Chami, and Mahesh (2019)

Unfortunately, gendered social norms and patriarchal tendencies create a stigma that is associated with experiencing violence and with reporting violent experiences (Devika et al. 2019). These cultural norms render survivors with limited ability to report, either because they would not be taken seriously (Devika et al. 2019) or because experiencing violence is seen as a private matter (Randhawa 2010). Thanks to the low social capital of women and girls, gaining strong family support, especially from male relatives, is often the only way they can formally report technology-facilitated GBV to law enforcement or access formal response mechanisms (Devika et al. 2019). However, some women report difficulty in being able to convince family members that they are being harassed:

“Sometimes it works when you stop telling him to leave you alone and instead put up the irritating chats and messages on your page, clearly saying that this guy is harassing you and if any kind of bad
Conservative cultural mechanisms also create an environment where LGBTQI+ individuals are discouraged from reporting due to fears of being outed (Devika et al. 2019; Gurumurthy, Vasudevan, Chami, and Mahesh 2019) and where girls are worried their sexual relationships will be exposed to their families or authorities (Padte 2014; Gurumurthy, Vasudevan, Chami, and Mahesh 2019). Several articles report that women feared their harassers were male family members, which again impeded reporting (Devika et al. 2019; Gurumurthy, Vasudevan, Chami, and Mahesh 2019). In addition, survivors are concerned that their phones or other electronics will be confiscated, either by police, a parent, or family member (Gurumurthy, Vasudevan, and Chami 2019; Ramaseshan et al. 2019; Kovacs, Padte, and SV 2013), or that their digital information would be leaked (Devika et al. 2019; Chowdhury 2016). The consequence of this would lead to punishment and/or their public lives being on display (Gurumurthy, Vasudevan, Chami, and Mahesh 2019).

Unlike adult survivors, research showed that adolescents wanted to talk to their parents about online issues, but that few actually do (Bhat et al. 2017). This is because most parents lack the awareness of the risks of ICTs and how to prevent their children from engaging in cyberbullying or being cyber victimized, preventing the possibility of support or engagement (Fitriana, Souket, and Yie 2020). Several sources also note poor overall parent-child communication as a key driver of children’s increased online presence (Gurumurthy, Vasudevan, Chami, and Mahesh 2019; Wachs et al. 2016; Fitriana, Souket, and Yie 2020; Le 2020; Bhat et al. 2017).

Since survivors rarely find support from their families, they instead turn to their friends and peers, both in person and online (Hassan, Unwin, and Gardezi 2018; Sittichai 2014; Sambasivan et al. 2019; Devika et al. 2019; Gurumurthy, Vasudevan, Chami, and Mahesh 2019). Friends are found to be a common source of support for women when experiencing online violence, especially for young women (Gurumurthy, Vasudevan, and Chami 2019; Kovacs, Padte, and SV 2013). Women have also used their online communities to generate responses and bring awareness to sexist social constructs that perpetuate online violence in hopes of preventing it in the future. Social media campaigns can bring awareness to online harassment, open up communication for women to access support and response mechanisms, and work to prevent future online violence (Arora and Scheiber 2017).

Together, women can find a sense of collective power to generate a response against their harassers. A story told in a 2019 focus group discussion highlights this: a group of women students in India were staying in a hostel when a harasser obtained their photos, uploaded them online, and began making obscene comments on them. Instead of blaming one another, the women came together to formally bring their complaint to the cyber police as a group. The police took action against the abuser (Devika et al. 2019).

**INDIVIDUAL BEHAVIOR MODIFICATION**

Due to insufficient institutional, social, and government support, as well as patriarchal cultural norms that make reporting and receiving support difficult, survivors are most often forced to protect themselves. One way survivors do this is by modifying their online behaviors. There is a strong gender component to altering online behaviors, with most studies reporting about how women and girls block
and refrain from online activities. Several studies note that women and girls tend to withdraw from social media sites after experiencing online violence more often than men and boys (Nova et al. 2019; Arora and Scheiber 2017; Ghazali and Ghani 2018; Sarkar and Rajan 2021), with some arguing this is furthering the gender digital divide (Nova et al. 2019).

Minimal modification of online behaviors include keeping settings and location on private, not uploading pictures and, for example, in Bangladesh, India, and Pakistan, using non-face alternatives like animals or landscapes (Sambasivan et al. 2019); being careful about updating status; not accepting friend requests from strangers or giving out any personal information; logging out after each use; only reading content and responses from known and verified accounts; and blocking messages and certain accounts. More severe forms of modification include survivors practicing self-censorship, content reduction, limiting content engagement, and changing email and phone numbers on profiles (Sambasivan et al. 2019; Sittichai 2014; Sarkar and Rajan 2021; Gudipaty 2017). Quitting online participation entirely, or at least no longer engaging with certain sites, was commonly mentioned:

“Most women survivors of cyber violence, in this study [in India], discussed how cyber violence forced them to quit participating online. Few survivors stopped for a year while others stopped for a few months. Certain survivors also stated that they have become dormant online and try to be careful about what they post.” –Sarkar and Rajan (2021)

In most cases in Asia, the onus is on survivors to quickly recover from an experience of technology-facilitated GBV, often by minimizing and normalizing it. In addition, due to patriarchal norms, research often notes that women have to be more careful than men in how they behave online:

“They [survivors in Pakistan] emphasized that they were careful in what they posted on social media, but that it was more important for women to be careful than men because of the nature of Pakistani society.” –Hassan and Unwin (2017)

In fact, study respondents and, at times, article authors spoke about these experiences with judgment about how survivors should behave online, both before and after an experience of violence:

“They [respondents in Malaysia] believe most crimes involving young women in social media took place due to the carelessness of victims for trusting strangers that they meet on social media.” –Ghazali and Ghani (2018)

While online behavior modification is commonly used as a self-preservation tactic, many articles also explain that survivors of technology-facilitated GBV often take no action as a result of their experience (Kovacs, Padte, and SV 2013; Hassan and Unwin 2017; Gurumurthy, Vasudevan, Chami, and Mahesh 2019), refraining from seeking social or logistical support or changing online behaviors. During FGDs, female college students in India shared how when sexist content is forwarded to them or how when they come across such content on Facebook, they choose to ignore it because speaking up could make them vulnerable to attack (Gurumurthy, Vasudevan, Chami, and Mahesh 2019).

**RECOMMENDATIONS**

Addressing technology-facilitated GBV in Asia requires collective action from multiple actors at the global, state, and local levels. The following recommendations are informed by findings from the
literature review, findings from case studies, and key informant interviews (KIs) with relevant stakeholders in Bangladesh, India, Indonesia, and Thailand. The recommendations are broadly applicable to the Asian continent and actionable upon country-specific operationalization. They include recommendations for national and local governments in Asia, tech companies, global organizations, and researchers. Recommendations are separated in a way that clearly defines major areas to address in Asia, but some may benefit from multiple actors working together to enact them. Some of these recommendations have been noted previously but are repeated in this report as they are necessary elements to addressing technology-facilitated GBV and have specific applications to Asia.

**POLICY RECOMMENDATIONS FOR LOCAL/NATIONAL GOVERNMENT**

- **Conduct an analysis of the legal landscape from a survivor and human rights–centered lens.** To best understand the strengths and gaps in national policy, a third-party gender analysis of the current laws and policies should be conducted by organizations specializing in technology-facilitated GBV and human rights to ensure transparency. Assessments should focus on whether current laws address different forms of technology-facilitated GBV, represent the interests of survivors, and are easy to enforce. Laws should also be analyzed using a human rights standard to assess if they target and punish vulnerable populations for consensual sexual expression (such as the LGBTQI+ community in Indonesia) or use these laws to unduly suppress dissent or free speech (for example, the Digital Security Act of 2018 in Bangladesh).

- **Enact laws specific to technology-facilitated GBV.** Laws addressing technology-facilitated GBV in many Asian countries are embedded in other laws, such as IT Acts. Relying on policies scattered across amended laws is confusing in prosecution and lacks comprehensive recourse for all of the varying forms of technology-facilitated GBV. Laws addressing technology-facilitated crime (such as India’s Information Technology Act of 2000, which focuses largely on commerce) lack a gendered element to the crimes, leaving out major protective elements when it comes to addressing technology-facilitated GBV (Pawar and Sakure 2019). Laws specific to technology-facilitated GBV can provide comprehensive and accessible protection for those being targeted.

- **Assess and amend/repeal anti-obscenity and anti-pornography laws that are actively harming survivors or restricting consensual sexual expression.** Multiple countries in Asia, such as Indonesia and India, have laws or policies that reinforce harmful gender norms by dictating acceptable social behavior from a patriarchal lens (Kamilia 2021; Xu 2010). These laws don’t support survivors; instead, they are used to actively punish them or to target and persecute vulnerable populations, such as those in the LGBTQI+ community (Kamilia 2021; Xu 2010). Laws should be assessed with a critical eye on how they negatively affect those experiencing technology-facilitated GBV. These laws may be embedded or intertwined with other protective measures, such as laws against child pornography, and therefore should be evaluated on a country basis to ensure necessary protective elements remain intact.

- **Conceptualize and circulate clear definitions of and information about technology-facilitated GBV with law enforcement and legal officials.** Technology-facilitated GBV is still a relatively new phenomenon, with varying terminology and conceptualizations of violence, which causes confusion on what it is and how to prosecute it. National governments need to generate a standardized definition among law enforcement and legal officials, which will enable them to clearly identify and address crimes that are considered technology-facilitated GBV. Law enforcement and legal officials must also be trained on what types of documents or media files are admissible as
evidence under these definitions in technology-facilitated GBV cases to prevent uneven applications of the laws.

- **Increase capacity for existing independent state bodies/organizations with a focus on technology-facilitated GBV.** Country governments should establish commissions on GBV with a department focusing specifically on technology-facilitated GBV, and/or they should create strong partnerships with national organizations already working to combat technology-facilitated GBV. Strong financial investments in these bodies and organizations should be made to ensure they have the capacity to address this growing phenomenon. International governments or global organizations may also serve as strong financial partners.

- **Repeal transphobic and homophobic legislation and strengthen protections for the LGBTQI+ population.** Criminalizing a person based on their gender or sexual identity or not protecting them against violence and discrimination reinforces social cues that those who do not conform to heteronormative cisgender binaries are deviants deserving of punishment. Transphobic and homophobic legislation (or lack of protective legislation) not only strengthens patriarchal norms that drive technology-facilitated GBV but increases the vulnerability of those belonging to the LGBTQI+ population as targets for online and offline violence, normalizing and perpetuating the phenomenon of violence based on identity.

### PROGRAMMING RECOMMENDATIONS FOR LOCAL/NATIONAL GOVERNMENTS AND CIVIL SOCIETIES

- **Conduct public education campaigns on technology-facilitated GBV.** Social understanding of technology-facilitated GBV is varied, and the many terms used to discuss the phenomenon can create difficulties in recognizing it in everyday life. In fact, many people still do not fully understand what is considered a crime: 72 percent of women in Pakistan are unaware of *Pakistan’s Prevention of Electronic Crimes Act 2016* (Aksar et al. 2020). Broad educational campaigns should focus on disseminating information on the definition of technology-facilitated GBV and its forms, as well as providing clear directives on how to report these crimes to the police and to non-profit organizations for those who don’t feel comfortable filing a police report. Public education programming should be offered using both online and offline education tools to ensure wide accessibility.

- **Develop specialized training for law enforcement and legal officials.** Sources in various countries throughout Asia have noted that those facing technology-facilitated GBV are often afraid to report to police due to fear of victim blaming or persecution by police. Law enforcement and legal officers, including lawyers and judges, should receive mandatory and recurring comprehensive training on gender awareness, GBV and technology-facilitated GBV, applicable laws, and appropriately interacting with survivors. Technology-facilitated GBV-centered police units should be developed where possible, and all officers should receive specialized training regardless of the existence of these units to quell them from reinforcing harmful gender norms and further silencing victims.

- **Introduce robust programming to change gender norms.** Attitudes and responses to technology-facilitated GBV are widely influenced by patriarchal cultural norms that reinforce victim blaming mentalities. Context-specific gender norms change programming should be aimed at all genders across multiple age groups. Programming should include—but not be limited to—discussions on gender equality, respecting boundaries and consent, dispelling common rape myths, responding to a friend or family member who has been assaulted, LGBTQI+ equality and rights, and
sexual and reproductive health and education. These programs can be introduced in schools and workplaces, as well as directly into the community in partnership with local non-profit or community outreach organizations.

- **Enhance data collection by streamlining reporting processes for survivors.** Accessible and anonymous reporting options should be made available in order to gain accurate data that are necessary to understand the depth and breadth of technology-facilitated GBV and create evidence-based, actionable change for prevention, mitigation, and response. Data collection should have both online and offline options to ensure accessibility for survivors who no longer feel comfortable with online spaces. Local government authorities, NGOs, community outreach organizations, and law enforcement officials can coordinate efforts to enhance and spread awareness about anonymous reporting mechanisms, both online and offline.

- **Launch digital literacy and online safety training.** Given the significant gaps in digital literacy across Asia, especially for those in rural areas with poor access to the internet, users often spread or share content with little understanding of how it might circulate across the internet. Digital literacy training can be done in partnership with schools, non-profits or community outreach organizations, and tech companies to generate awareness in the community (especially among young users) and teach appropriate online behavior. These training sessions should include topics such as navigating privacy settings, establishing and respecting consent in online spaces, understanding technology-facilitated GBV, and how shared images and information are used online. Digital literacy training should be viewed as an integral part of any efforts to build or integrate digital technology into society, especially when used to close the gender digital divide.

- **Develop trauma-informed best practice training for workplaces or organizations with high-risk employees or members.** Individuals whose job or affiliation requires them to operate in the public eye face a high risk of experiencing technology-facilitated GBV. This includes politicians, journalists, activists, and community leaders who are seen widely on the internet and may be targeted due to their gender, ethnicity, religion, sexual orientation, or other identity factors. Best practice training and resources should be developed for such organizations or workplaces to ensure they are capable of providing necessary support and protection to high-risk employees. Trainings should further educate employees on the current laws and avenues for recourse available to those experiencing technology-facilitated GBV.

**RECOMMENDATIONS FOR TECHNOLOGY COMPANIES**

- **Enhance accessibility of privacy settings.** Users should have easy access to privacy information in languages they can understand. Currently, many platforms only have this information available in a few major languages. The design of privacy settings should be streamlined and made user-friendly. Advanced privacy settings should be the default option when apps are downloaded or online profiles are created. Social media and apps should have easy-to-locate and step-by-step directions to enhance or update privacy settings.

- **Review online community standards to ensure gender and context are taken into consideration.** What may not be considered abusive, violent, or offensive in one context might be so in another or be done with malicious intentions to cause personal or social harm, resulting in significant repercussions for survivors. This context can easily be lost or ignored when reporting these incidents to technology companies. One example of this is the reporting of image-based abuse: for instance, releasing (without consent) a fully clothed photo of a woman would not be categorized
as abuse by many technology company reporting systems. Yet, in some Asian contexts, this is considered highly personal and sensitive and could cause significant damage to a woman’s reputation (Gurumurthy, Vasudevan, and Chami 2019). Technology companies should consider the malicious intent to harm when assessing unacceptable content rather than solely assessing the image itself.

- **Strengthen staff capacity to improve response mechanisms and support resources for survivors.** While technology companies have increased reporting mechanisms, there is still a major gap between the resources and support they provide to those experiencing technology-facilitated GBV. Companies are not well equipped to handle reports in many languages other than English (Gurumurthy, Chami, and Vasudevan 2017). The COVID-19 pandemic has exacerbated this resource gap, putting greater strain on staff trying to address misinformation on their platforms as well as the significant rise in technology-facilitated GBV. Simultaneously, the pandemic has also provided impetus for technology companies to put more effort, resources and expertise into content moderation, indicating that, in addition to increased need, there is now more will and opportunity to increase capacity for such activities. Technology companies must build their capacities to ensure timely and proper response to harmful content, violent behavior, and reports of perpetrators. Capacity building should include strong financial investments into growing available staff, training staff on recognizing harmful gender norms, and working closely with intermediaries who can provide localized language and cultural support.

- **Invest in trauma-informed and transparent reporting and response mechanisms.** Considering the high amount of technology-facilitated GBV on social media sites across Asia, strategic investments should be made into dedicated technology-facilitated GBV prevention and response mechanisms that are widely available to users. Reporting mechanisms should be available in multiple languages and developed with trauma-informed professionals to ensure they do not retraumatize survivors. Technology companies should partner with national organizations combating technology-facilitated GBV, offering survivors links directly to support pages or anonymous reporting structures to enhance data collection and data sharing efforts nationally. Companies should further invest in trauma-informed resources developed in collaboration with organizations specialized in supporting survivors of technology-facilitated GBV (such as the recent partnership between dating app Bumble and remote trauma therapy service Bloom by Chayn). Finally, companies should enhance transparency by regularly publishing reporting data.

**RECOMMENDATIONS FOR RESEARCHERS**

- **Increase focus on Central Asia and Pacific Islands.** While there is a need to increase overall research across Asia, this literature review found significant gaps in research on technology-facilitated GBV, specifically in Central Asia and Pacific Islands. In addition to continued research across the region, strong investments should be made to conduct primary research in these regions.

- **Strengthen research partnerships with those responsible for reporting mechanisms and data collection.** Due to factors such as fear of reporting and inaccessible reporting mechanisms, much is still unknown about how vastly technology-facilitated GBV affects countries in Asia and who is affected by it. Limited reporting leads to gaps in information about perpetrators, including who they are and why they commit technology-facilitated GBV. Programmatic efforts to enhance anonymous and accessible reporting structures should be paired with research to generate nuanced, country-specific understanding of perpetrator and victim profiles, most prevalent forms of technology-facilitated GBV, and websites or social media where it occurs frequently.
• **Investigate social media’s role in facilitating and addressing technology-facilitated GBV.** Technology-facilitated GBV is highly prevalent on global social media platforms, including Facebook, Twitter, WhatsApp, TikTok, YouTube, and Instagram. Yet, these platforms have struggled to respond to this phenomenon. Further research should be done to understand how social media perpetuates technology-facilitated GBV and what tech companies can do to address and prevent it.

• **Increase knowledge of survivor-centric and culturally-nuanced responses.** Those facing technology-facilitated GBV experience a number of impacts, including emotional and psychological trauma. In-depth studies should be conducted on response and mitigation efforts, legal application, and culturally nuanced survivor support resources. These studies can support tailored programming considering the type of violence.

• **Examine the gendered impact in areas or sectors with burgeoning technology growth.** Typically, rural jobs in Asia—such as farming—have largely functioned offline. However, as technology grows to be a larger part of global daily life, such as increases in internet access and smartphone usage, it is becoming a greater source of information for workers in these roles. Investigating the increasing role of technology and the gendered impacts of it can provide insight for early intervention and prevention of technology-facilitated GBV as well as opportunities to incorporate digital literacy training that can aide in closing the gender digital divide.

• **Investigate trauma-informed best practices between employers and employees.** With the growth of the internet and remote work during COVID-19, many workplaces have increased their online presence (i.e., mandatory online bios/photos, recorded meetings or webinars, and social media updates). Personal online presence has become the norm in many workplaces, and consent for publishing personal information online is often assumed. Research focused on the experience of employees who have faced technology-facilitated GBV and investigation of trauma-informed best practices for workplaces using online spaces can bring greater awareness and prevention to technology-facilitated GBV for employees.

**CONCLUSION**

The landscape analysis reveals key trends and gaps related to technology-facilitated GBV in Asia. As noted in this review, this form of violence is shaped not only by societal and gender norms, but also influenced by the ever-evolving technological landscape within the region. Women, girls, gender and sexual minorities, and those with intersecting marginalized identities are reportedly more vulnerable to experiencing both online and offline violence, have longer-lasting impacts, and are less likely to share or report their experience.

Although there is growing interest among implementers and policy-makers to address this pervasive yet relatively unexplored issue, there remain significant gaps in prevention and response mechanisms, which underscores the need to implement some of the recommendations proposed above. The urgency to address prevention, mitigation and response barriers is particularly important considering the dynamic and quickly changing landscape of technology-facilitated GBV. As new trends emerge, in tandem with the development of new technologies, the lack of policy and programming around this issue further compounds the problem. There is a need for an urgent and concerted effort by key stakeholders including technology companies, government and law enforcement authorities, civil societies, and academic researchers to develop and implement timely and nuanced solutions.
4. REFERENCES


Balakrishnan, V. “Cyberbullying among Young Adults in Malaysia: The Roles of Gender, Age and Internet Frequency.” Computers in Human Behavior 46 (2015): 149–57. https://doi.org/10.1016/j.chb.2015.01.021


Haarr, Robin N. “Assessment of Violence Against Children in Schools in Kazakhstan.” UNICEF, 2013. https://www.unicef.org/kazakhstan/media/2076/file/%D0%9F%D1%83%D0%B1%D0%BB%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F%20%D0%BD%D0%B0%20%D0%BD%D0%B3%D0%BB.pdf


Panchanadeswaran, S., A.M. Unnithan, S. Chacko, M. Brazda, and S. Kuruppu. “What’s Technology Got to Do with It? Exploring the Impact of Mobile Phones on Female Sex Workers’ Lives and Livelihood in


ANNEX A, RESEARCH QUESTIONS

The research team developed priority research and sub-research questions in collaboration with USAID to guide the research process. Given the paucity of evidence on this nascent topic, the research questions focused on descriptive categories such as trends, profiles of survivors and perpetrators, and the impacts of experiencing such violence and harassment.

RESEARCH QUESTION 1: What is technology-facilitated GBV?

Sub-question 1.1: What are the common forms of technology-facilitated GBV?

Sub-question 1.2: What platforms are typically used to perpetrate technology-facilitated GBV?

Sub-question 1.3: What are the reported incidence and prevalence rates of technology-facilitated GBV in the Asia-Pacific region?

RESEARCH QUESTION 2: What are the Asia-Pacific regional trends and perceptions related to technology-facilitated GBV?

Sub-question 2.1: How has the incidence/prevalence changed over time?

Sub-question 2.2: What are in-country or regional perceptions of technology-facilitated GBV?

RESEARCH QUESTION 3: What does perpetration look like in the Asia-Pacific Region?

Sub-question 3.1: Are there any gender and age differences among perpetrators depending on the forms of GBV perpetrated?

Sub-question 3.2: What are the motivations and intentions for perpetuating GBV?

Sub-question 3.3: What factors incentivize technology-facilitated GBV?

RESEARCH QUESTION 4: What does survivorship/victimization look like in the Asia-Pacific Region?

Sub-question 4.1: Are there any gender and age differences among survivors depending on the forms of GBV experienced?

Sub-question 4.2: How does technology-facilitated GBV impact different types of individuals?

RESEARCH QUESTION 5: What are the impacts of technology-facilitated GBV, and how do individuals seek help and support?

Sub-question 5.1: How does technology-facilitated GBV impact individuals physically, psychologically, social, economically, functionally, and aspirationally?

Sub-question 5.2: What are the help-seeking behaviors that individuals engage in to address and mitigate tech-facilitated GBV, including how individuals modify online behaviors?
Sub-question 5.3: What (if any) is the correlation between in-person violence and technology-facilitated GBV?

**RESEARCH QUESTION 6:** How are different groups and actors responding to technology-facilitated GBV?

Sub-question 6.1: What is the response of family and community members?

Sub-question 6.2: What is the response of schools?

Sub-question 6.3: What is the response of technology companies?

Sub-question 6.4: What is the response of employers?

Sub-question 6.5: What is the response of local and government authorities?
## ANNEX B, TERMS FOR SEARCH STRATEGY

### CONSTRUCTS OF TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE

<table>
<thead>
<tr>
<th>Tech-Facilitated</th>
<th>Violence</th>
<th>Gender + Sexuality</th>
<th>Gender + Violence</th>
<th>Tech-Facilitated + Violence</th>
<th>Tech-Facilitated + Gender-Based Violence</th>
<th>Asia-Pacific Region&lt;sup&gt;4&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology</td>
<td>Violence</td>
<td>Gender</td>
<td>Sexism</td>
<td>Trolling</td>
<td>“Revenge Porn”</td>
<td>Asia</td>
</tr>
<tr>
<td>Cyber</td>
<td>Abuse</td>
<td>Women</td>
<td>Homophobia</td>
<td>Doxing</td>
<td>Upskirting</td>
<td>Central Asia</td>
</tr>
<tr>
<td>Online</td>
<td>Harassment</td>
<td>Girls</td>
<td>Sextortion</td>
<td>Hacking</td>
<td>Downblousing</td>
<td>South Asia</td>
</tr>
<tr>
<td>Internet</td>
<td>Aggression</td>
<td>Female</td>
<td>Exploitation</td>
<td></td>
<td></td>
<td>Southeast Asia</td>
</tr>
<tr>
<td>Digital</td>
<td>Victimization</td>
<td>Intimate Partner</td>
<td>IPV</td>
<td></td>
<td></td>
<td>Pacific Islands</td>
</tr>
<tr>
<td>Mobile</td>
<td>Bullying</td>
<td>Dating</td>
<td>VAWG</td>
<td></td>
<td></td>
<td>---------</td>
</tr>
<tr>
<td>ICT</td>
<td>Stalking</td>
<td>Sexual</td>
<td>VAW</td>
<td></td>
<td></td>
<td>Afghanistan</td>
</tr>
<tr>
<td>Electronic</td>
<td>Exploitation</td>
<td>LGBTQI+</td>
<td></td>
<td></td>
<td></td>
<td>Bangladesh</td>
</tr>
<tr>
<td>Social Media</td>
<td>Threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cambodia</td>
</tr>
<tr>
<td>Media</td>
<td>Hate Speech</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>India</td>
</tr>
<tr>
<td>Image Based</td>
<td>Impersonation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Indonesia</td>
</tr>
<tr>
<td>Gaming</td>
<td>Rape</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Kazakhstan</td>
</tr>
<tr>
<td>Sexting</td>
<td>Trafficking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Kyrgyz Republic</td>
</tr>
<tr>
<td></td>
<td>Nonconsensual</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Laos</td>
</tr>
<tr>
<td></td>
<td>Defamation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Myanmar</td>
</tr>
<tr>
<td></td>
<td>Libel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Nepal</td>
</tr>
<tr>
<td></td>
<td>Slander</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Pakistan</td>
</tr>
<tr>
<td></td>
<td>Shaming</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Papua New Guinea</td>
</tr>
<tr>
<td></td>
<td>Insults</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sri Lanka</td>
</tr>
<tr>
<td></td>
<td>Teasing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Tajikistan</td>
</tr>
<tr>
<td></td>
<td>Masquerading</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Timor-Leste</td>
</tr>
<tr>
<td></td>
<td>Swatting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Vietnam</td>
</tr>
<tr>
<td></td>
<td>Catfishing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

<sup>4</sup> This list only includes USAID priority countries but the peer-reviewed search includes other countries in Central, South and Southeast Asia, as well as the Pacific Islands classified by the World Bank as low and middle-income. These include Bhutan, Fiji, Kiribati, Malaysia, Maldives, Marshall Islands, Micronesia, Philippines, Samoa, Solomon Islands, Thailand, Tonga, Turkmenistan, Tuvalu, Uzbekistan and Vanuatu.
ANNEX C, METHODS AND LIMITATIONS

PEER-REVIEWED LITERATURE

To extract peer-reviewed articles that align with the scope of this research, we searched PubMed, Scopus, and Web of Science databases. We started by developing a search string (see Annex A) to capture articles related to technology-facilitated GBV, which was then entered into the three databases with appropriate database-specific syntax. To add further rigor to our search approach and to ensure that our search string was generating relevant articles, the team checked the query results to see if the search string generated five “test” articles identified by the team. We uploaded query results to Covidence, a systematic review software, where we conducted multiple levels of screening. First, we screened query results by title and abstract based on the inclusion/exclusion criteria. Two team members screened each article, and a third team member who did not conduct the first round of screening resolved all screening conflicts. Then, peer-reviewed articles that were selected during the title-abstract round of screening were further screened by reading the full-text of the article. The research team collectively resolved any conflicts that arose during the full-text screening stage. Finally, peer-reviewed articles that were shortlisted after both stages of screening were extracted from Covidence and uploaded to Dedoose, a qualitative analysis software, where articles were coded using a detailed codebook iteratively developed by the team.

To keep our review focused and manageable, we identified the following inclusion and exclusion criteria:

**Inclusion Criteria:** peer-reviewed literature on technology-facilitated gender-based violence

- Published in English.
- Published between 2006–2021.
- Published with an explicit emphasis on the Asia-Pacific region, specifically low- and middle-income countries in Central, South and Southeast Asia, and Pacific Islands. The country/region of interest must appear in the title or abstract (see framework for exact list of countries).
- Published with an explicit emphasis on technology-facilitated violence. A tech term from the search term framework must appear in the title or abstract.
- Published with an explicit emphasis on gender. A gender term from the search term framework must appear in the title or abstract.

**Exclusion Criteria:** Articles that do not meet the above criteria were discarded. In addition, articles on the following topics were excluded as they were deemed out of scope.

- App-based technologies, groups on social media, and online campaigns (e.g., #metoo) designed to ensure women’s safety since they are focused on tech-based solutions for GBV prevention rather than how technology is used to perpetuate GBV.
- Using technology to determine the sex of a fetus and aborting a pregnancy if it is a girl. Even though this technically fits our definition of technology-facilitated GBV, it is not part of the usual discourse on this topic and is treated as a separate issue in much of Asia.
- Gender discrimination faced by women attempting to conceive using assisted reproductive technology.
• Gender differences in access to technology and technology-related services (health care, education, etc.).
• Tech interventions or services that unintentionally put women at increased risk of violence (e.g., radio messaging intervention designed to increase contraceptive uptake had unintended consequences because women who participated in this faced increased incidence of intimate partner violence (IPV).
• Policy-focused documents.

GREY LITERATURE

To address the research questions through a review of grey literature, the research team adopted two main approaches. The first approach was a database and Google search, which included searching databases related to organizations affiliated with the GBV space and international portals. Google was used to support the search process given varying database functionality, e.g., producing mostly irrelevant hits or when the hits were not enumerated. The search process was designed to be highly iterative and flexible to account for the challenging search functionality of organizational websites and extract documents such as reports, research or policy briefs, presentations, dissertations, conference abstracts, requests for proposals, white papers, and toolkits.

The research team developed a list of 27 relevant organizations and portals. For each organization and portal, the team entered the search terms into the search function, scanned the titles of extracted documents, reviewed the executive summaries, abstracts, or skimmed full texts of relevant documents, and maintained a list of relevant documents for further assessment in an Excel document. The team conducted this process up through the first 10 pages of search results. To supplement this process, the team conducted a Google search using key search terms and the name of the organization or portal, using the same review procedures. A total of 65 articles were initially extracted for full text review. The team evaluated the full texts of the extracted documents for relevancy based on inclusion and exclusion criteria. After removing 2 duplicates, 7 peer-reviewed articles, and 19 articles that did not meet the inclusion criteria, a total of 37 documents were included for coding. During the coding process, 4 documents produced no codes and were subsequently excluded from analysis. The final number of grey literature articles included for analysis was 33.

The second approach for searching grey literature entailed a thorough search of USAID's Development Experience Clearinghouse (DEC) to identify documents such as request for proposals (RFPs), annual reports, evaluation reports, and other such documents that meet the inclusion/exclusion criteria indicated below. Based on our search string, the DEC yielded 156 articles, of which 40 were removed after adjusting for date range, 42 adjusted for geographic scope, 6 were removed after deleting duplicates, and 65 were removed after title screening—leaving us with 3 articles that were included for final analysis.

The research team applied the same inclusion and exclusion criteria for the grey literature as for peer-reviewed literature, with the exception of:

• Regional focus was limited to USAID priority countries in the Asia-Pacific region (Afghanistan, Bangladesh, Burma, Cambodia, India, Indonesia, Kazakhstan, Kyrgyz Republic, Laos, Nepal, Pakistan, Papua New Guinea, Sri Lanka, Tajikistan, Timor-Leste, and Vietnam).
• Peer-reviewed articles, media and news articles, and blog posts were excluded.
LIMITATIONS

Given the scope and research objectives of the study, the research team screened out articles that did not have an explicit reference to technology-facilitated violence, gender/sexuality, or region/country of interest in the title or abstract. Consequently, it is possible that some articles on this topic were not included in the study even though they might have referenced these terms in the full text. The research team agreed that if technology-facilitated GBV was the focus of the study, the relevant terms would be covered in either title or abstract, if not both.