Editors: Heather Richter Lipford, richter@uncc.edu | Jessica Staddon, jessica.staddon@gmail.com

Toward Gender-Equitable Privacy and Security in South Asia

Nithya Sambasivan | Google
Nova Ahmed | North South University
Amna Batool | Information Technology University
Elie Bursztein and Elizabeth Churchill | Google
Laura Sanely Gaytán-Lugo | Universidad de Colima
Tara Matthews | Independent Researcher
David Nemer | University of Virginia
Kurt Thomas and Sunny Consolvo | Google

South Asia has one of the world's largest populations—India, Pakistan, and Bangladesh alone are home to more than 20% of all people. The region is also one of the fastest-growing technology markets as a result of its increased infrastructure and growing affordability. Despite this progress, South Asia faces one of the largest online gender disparities in the world, i.e., women are 58% less likely to connect to the mobile Internet than men.[1] We believe that, as the Internet becomes more globally accessible, it is imperative for technologists to intentionally examine the biases and inequities perpetuated in technology to truly enable gender equity online.

For South Asian women, a major challenge confronting meaningful online participation is ensuring one's privacy and safety.[1,4] For cultural and economic reasons, South Asian women often share their devices with family members; e.g., gender norms may lead to a mother sharing her phone with her kids (whereas the father may not).[5] Today's features, settings, and algorithms do not cater well to such an on-device privacy model in shared device situations.

Abuse on applications and platforms also poses potentially life-threatening risks and prohibits women from participating online in South Asia. For instance, Qandeel Baloch, a social media celebrity in Pakistan, was murdered by her brother for posting selfies online.[6] In a separate event, a 21-year-old woman in India committed suicide after her social media profile photo was stitched to a seminude body and spread virally.[7] While online abuse is not limited to South Asian women, the risks are often heightened for this community due to the influence of patriarchal norms and because fewer women are online.

In this article, we highlight the privacy and safety experiences of women across India, Pakistan, and Bangladesh. Based on a qualitative research study, we summarize the online privacy and safety challenges women face today and propose technology recommendations for addressing them. When designing and implementing technologies, we ask readers to consider these persistent, everyday threats faced by South Asian women to help ensure that everyone can safely participate online.

Methodology

Between 2017 May and 2018 January, we conducted semistructured, in-person interviews and focus groups with 199 participants who identified as women living in India, Pakistan, and Bangladesh (11 participants identified as queer, lesbian, and transgender male to female). We also interviewed six nongovernmental organization (NGO) staff members working in the area of women's safety and LGBTQ rights. The participants included college students, housewives, small business owners, domestic maids, village farm workers, IT professionals, bankers, small business owners, and teachers. Our interviews spanned 14 cities and rural areas, totaling 103 participants from India, 52 participants from Pakistan, and 44 participants from Bangladesh. We conducted interviews in participants' local languages. More details can be found in our previous publications.[8,9] All of the participant names presented in this article are pseudonyms.

Digital Object Identifier 10.1109/MSEC.2019.2912727
Date of publication: 9 July 2019

Device Privacy

Since I want to prevent my kids from using my phone, I use phone locks. But my kids open it each time I change it; they are too smart. I have to change my app lock PIN every week. —Jyoti, a 40- to 45-year-old housewife from Kanpur, India.

Device Sharing Is Common and Valued

Participants expressed a cultural expectation that they, because of their gender roles as caregivers, would regularly share their devices and digital activities with social relations in three main ways:

1. *Shared usage* refers to when children, family members, friends, or colleagues borrowed someone's phone. Women's mobile phones were often viewed as "family" devices.
2. *Mediated usage* is when someone sets up or enables a digital experience for a less-tech-confident user, often because of technology illiteracy or gender roles[4] (e.g., a daughter may search for and then play a video for her mother).
3. *Monitoring* refers to when someone else checks messages, content, or apps on a person's phone without otherwise needing to use the phone. Approximately half of the participants thought it was acceptable to have their phones monitored by others to avoid viruses or unwanted attention online, but the other half felt coerced.

Similar to Jeans and Dating: Privacy Has Value Connotations

Our participants perceived the term *privacy* in various ways. Some viewed it as a Western import, such as "jeans and dating," in direct opposition to their cultural ethos of openness. For example, we heard "privacy is not for me, it's for those rich women," among many lower- and middle-income participants, implying that privacy was for upper-class families where social boundaries were presumed to be acceptable.

Privacy-Preserving Practices in Device Sharing

Regardless of value assignments to privacy, all of the participants in our study—no matter their social or economic background—employed techniques that maintain a degree of privacy while sharing devices in line with local norms. These techniques included phone and app locks, content deletion, private modes, and technology avoidance (see Table 1).

Phone Locks

Participants regularly used PINs or pattern locks on their phones to prevent misuse by strangers or in case of theft. Phone locks, which were used by 58% of participants, can be an overt, effective strategy in many contexts; however, they were seldomly effective in preventing nearby family members or friends from accessing phones.

App Locks

Another commonly used, semiovert technique for privacy were app locks. These apps, used by 29% of the participants, give a user the ability to password- or PIN-protect specific applications, content, or folders. Participants reported that app locks provided more granular control than phone locks but didn't provide the secrecy from friends and family that they sometimes desired. The very presence of an app lock icon or login sometimes led to questions such as, "What are you hiding from me?"

Deletions

As a more covert action, participants deleted sensitive content from devices that traveled freely among various family members. This action included aggregate deletions of entire threads or histories of content as well as entity deletions of specific chats, media, or queries.

Sixteen percent of participants reported using aggregate deletions

Table 1. Participants' privacy-preserving practices in device-sharing situations, arranged from left to right by what participants perceived to be least-to most-effective.

Phone lock	App lock	Aggregate and entity deletions	Private modes	Avoidance
To prevent misuse by strangers or in case of theft	To secure specific content or apps from others	To remove individual (or a full history of) content or queries	To explicitly enter a mode before performing a sensitive activity	To not do something around family or in public or at all
Challenges ▪ People around the user can figure out PINs	**Challenges** ▪ People around the user can figure out PINs ▪ May lead to "sticky" situations	**Challenges** ▪ Discovery ▪ Awareness ▪ Complicated mental models	**Challenges** ▪ Awareness ▪ Usability ▪ Can be viewed as "shady"	**Challenges** ▪ Complicated mental models (cross-device actions) ▪ May limit access to tech

when they were unable to find a way to delete a specific piece of content, wanted a large amount of their content deleted (e.g., browsing history, search history, or message history), or believed that their phones were slowing down. Entity deletions were used by 64% of participants to remove individual items, such as a single text message, photo, or a previously searched term, to manage what others who shared or monitored their phones would see. In personalized systems, entity deletions were particularly challenging for many participants to discover and manage. For example, Shaina (a 35–40-year-old medical representative from Kanpur, India) described how she managed her recommendations through "algorithmic hacking": "When I watch a video that is little bit not nice, then I search for five or six other videos on different topics to remove it."

For details on additional privacy techniques, including private modes and avoidance, please see our paper that was presented at the 14th Symposium on Usable Privacy & Security.[8]

Online Safety

> *On social media platforms they say, "I love you," "Come with me." …. Recently, I posted a scooter ad on a classifieds app, and even there I got requests like, "Do you want to have sex?" —Shanti, a 25–30-year-old from Bangalore, India.*

Digital Abuse Is Commonly Experienced by Women in South Asia

A majority (72%) of our participants reported experiencing digital abuse, such as unwanted messages or nonconsensual release of their information, especially on social media platforms. Not only was abuse common, but these incidents severely harmed women's perceived integrity and honor, because in South Asia, the onus of a family or a community's reputation often rests on women. Women were often presumed by their communities to be complicit in the abuse.

Several of the abuse incidents occurred in hyperlocal communities where their tight-knit nature led to repercussions in the real world (such as domestic violence or losing marriage opportunities). The viral nature of abusive content on social media platforms further exacerbated the harms. Based on our interviews, we identified three main types of abuse (see Table 2).

Cyberstalking occurred when an abuser initiated unwanted contact (reported by 66% of participants). Participants reported receiving daily calls, friend requests, and direct messaging from unknown men (most of these were sexual in nature). The frequency of incidents was exacerbated in part by social platforms and communication tools that open new channels for connections and messages from strangers. Incidents included persistent "I love you" messages from strangers or unwanted contact via phone calls and short message services (SMSs). For instance, Mishita, a 20–25-year-old garment factory worker in Dhaka, Bangladesh,

Table 2. The threat model of online abuse types, harms, and coping methods among participants (arranged from left to right in high-to-low-reported incidences).

Cyberstalking	Impersonation	Personal content leakages
Undesired contact from strangers on platforms	Malicious likeness of the individual's identity, created or modified without consent	Nonconsensual exposure of interactions and content in unwanted social contexts
Mechanisms ▪ Friendship requests from strangers ▪ Unwanted SMSs and calls	**Mechanisms** ▪ Synthetic pornography ▪ Fake profiles	**Mechanisms** ▪ Nonconsensual sharing of photos, conversations, or identity
Harms ▪ Self-censorship and limited participation ▪ Physical violence ▪ Emotional damage	**Harms** ▪ Reputation damage ▪ Physical violence ▪ Emotional damage	**Harms** ▪ Reputation damage ▪ Physical violence ▪ Emotional damage ▪ Coercive romantic involvement
Coping practices ▪ Block requests ▪ Limit information online ▪ Use fake identities ▪ Check for mutual trust	**Coping practices** ▪ Proactively change profile photos to nonface images ▪ Support from family and friends ▪ Support from NGOs	**Coping practices** ▪ Support from family and friends ▪ Support from NGOs ▪ Support from police

reported that unwanted calls led to her parents suspecting her of engaging in relationships with men:

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

Impersonation involved an abuser creating a malicious likeness of an individual without his or her consent (15%). Incidents included synthetic pornography (e.g., stitching pornographic material to an individual's face) and stealing an individual's identity to create a false, disreputable profile. Participants were initially unaware that someone copied, manipulated, and reshared their personal content on social media platforms. It was not until after negative repercussions from their community surfaced that participants realized their identities had been misappropriated. Mariyam, an 18–25-year-old gym trainer in Lahore, Pakistan, was in the 12th grade when her profile photo and identity were stolen by an abuser to create a false, sexually revealing profile. She recalled how her male classmates made unexpected sexual overtures to her. Mariyam's school principal rebuked her "loose character" and blamed her family for raising a morally corrupt daughter.

Personal content leakages involved an abuser nonconsensually exposing the participant's online activity in unwanted social contexts (14%). Abusers turned ordinary interactions, such as friendly chats and normally innocent photos, into harmful content by leaking them in unwanted contexts, such as to participants' elderly relatives, employers, or the public and using them as blackmail. Content leaks were the most incapacitating form of abuse reported in our study, principally due to the damage they caused to participants' social reputation and dignity. For example, Chandra (a 25–30-year-old in Delhi, India) described threats received from a male stranger about cross-gender interactions, which were not always socially accepted: "[He said,] 'Talk to me every day or I will tell your family that you were talking to me.'"

Online Abuse Looks Materially Different in South Asia

Content that may not be sensitive or is only mildly sensitive in Western contexts was occasionally very sensitive to the women in our study: e.g., a photo of a fully clothed woman or a woman's name, when revealed in the wrong context, could lead to serious negative consequences for women in South Asia. As Raheela, an NGO staff member for a women's safety helpline in Pakistan, explained:

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

Furthermore, technology platforms were assumed to not consider South Asian cultural contexts when reviewing abuse complaints. Fully clothed photos, for example, may not violate platform policies, even if a harasser was using it to abuse someone. Review teams' limited understanding of local languages was cited as another challenge. When it came to reaching out to law enforcement for support, among those who had filed police complaints, paper evidence and victim blaming were seen as impediments to seeking help.

Online Abuse

Online abuse frequently led to serious consequences for women, such as emotional damage (55%) and reputation damage (43%), as well as coercive romantic involvement (5%) and domestic violence (4%). These could further result in adverse social gossip, loss of marriage opportunities, and exclusion from parent–teacher meetings.

Informal Support Versus In-App Reporting and Law Enforcement Support

Participants frequently coped with online abuse by relying on family and friends (47%). They also limited their online activities and used nonface photos for their profiles to help safeguard their online presence. They rarely leaned on technology platforms for abuse reporting (2%) or reached out to law enforcement (1%) for help.

Designing to Enable Gender Equity Online

Define Privacy and Counterabuse Policies in Locally Situated Ways

Our results point to the need for a culturally and infrastructurally sensitive understanding of perceptions, practices, and value systems of privacy and abuse. Close social relations are often a part of the assumed personal space of single-user applications, challenging prevailing technical assumptions on user identities, personalization models, and usage metrics.

Our participants had divergent views on how relevant the label of "privacy" was to them, underscoring the need for more research on privacy across different cultures. Although it may be tempting to conclude that our participants' limited autonomy with technology is problematic, when viewing from outside the cultural context, our participants had a range of views regarding monitoring and sharing. That women adopted diverse and sophisticated privacy-preserving

practices indicates a need for technology to be designed with shared-use scenarios as common, rather than as an edge case.

According to our findings, the abuse experienced by women in South Asia is materially different from what has been reported in other geographical or cultural contexts. Significant consequences resulted from what may seem like a minor infraction, such as a stranger lifting a participant's profile photo or leaking their name.

Formal support systems, such as law enforcement and in-app abuse reporting, were viewed by the women as largely unsupportive. Many participants were not aware when their digital identities were impersonated until they felt societal repercussions. NGOs acted as alternatives to formal systems, but they faced discovery issues. Overall, culturally sensitive formal recourse, technological safeguards, and in-app abuse handling, plus improved NGO discovery, could help South Asian women feel safer online.

Improve User Outreach on Privacy and Safety

Our research points to an opportunity for improving user education around existing privacy features. For instance, participants liked the concept of private modes, but these modes were rarely discovered or used. Promoting private modes in a culturally sensitive way may help more users benefit from them.

When it comes to counterabuse techniques in the South Asian context, any outreach must consider that a family and a community's reputation often rests on women, something that compounds the prevalence and consequences of abuse. Internet safety education aimed at families and young male users may be especially beneficial in the South Asian context.

Design and Algorithmic Considerations

Design considerations that improve device privacy may benefit many women. Deleting content, e.g., search queries and browser histories, was sometimes difficult for participants—improving affordances and user-interface responses could help. Implementing identity models for shared use could increase the comfort and utility of personalization systems.

In terms of counterabuse designs, it is important to offer flexibility in user identity models. Understanding and designing using local technology vernacular may make tools more approachable. Improving the discovery of in-app abuse reporting as well as takedown policies and responses can greatly enable user trust. Design principles from safe spaces, such as moderation and reinforcement of community guidelines, could also help. Such improvements can enable South Asian women to equitably participate and demand accountability online.

This article highlighted the privacy and safety experiences of South Asian women, in particular across India, Pakistan, and Bangladesh. Although this region is one of the fastest-growing technology markets, women are 58% less likely to connect to the mobile Internet than men. We examined the Internet privacy and safety experiences of women in these countries. We ask readers to consider the challenges, cultural expectations, and contexts they face so that South Asian women can safely participate online. ■

Acknowledgments

This article summarizes two papers previously published in the 2018 14th Symposium on Usable Privacy & Security[8] and the 2019 ACM Computer–Human Interaction Confererence on Human Factors in Computing Systems.[9] We thank the study participants, the nongovernmental organizations and research partners, and the article reviewers and editors. We are grateful to Asif Baki, Cary Bassin, Dan Russell, Dave Shapiro, Jess Holbrook, Jose Manuel Faleiro, Lawrence You, and Patrick Gage Kelley for their support. We also thank our collaborators: Aimen Shah, Beenish Fatima, Cheng Wang, Chetna, Garen Checkley, Maham Javaid, Muhammad Salman Khalid, Oxana Comanescu, Rahat Jahangir Rony, Rahath, Sarah Shoilee, Shahreen Psyeche, Silvia Ahmed, Syeda Khan, Syeda Tanvir Mushfique, Tallal Ahmed, Taylor Marable, and Zaheer Sarwar.

References

1. O. Rowntree. (2019). The mobile gender gap report. GSMA. London, U.K. [Online]. Available: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/GSMA-Connected-Women-The-Mobile-Gender-Gap-Report-2019.pdf
2. Census of India. 2011. Accessed on: May 10, 2019. [Online]. Available: http://www.censusindia.gov.in/2011census/F-series/F-1.html
3. Bangladesh Bureau of Statistics. 2019. Accessed on: May 16, 2019. [Online]. Available: http://www.bbs.gov.bd/
4. GSMA. "Bridging the gender gap: Mobile access and usage in low-and middle-income countries," 2015. [Online]. Available: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/02/Connected-Women-Gender-Gap.pdf
5. N. Sambasivan, E. Cutrell, K. Toyama, and B. Nardi, "Intermediated technology use in developing communities," in *Proc. ACM Special Interest Group Computer–Human Interaction (SIGCHI)*, 2010, pp. 2583–2592.

6. I. Gabol and T. Subhani, "Qandeel Baloch murdered by brother in Multan: police," *Dawn*, July 16, 2016. [Online]. Available: https://www.dawn.com/news/1271213/qandeel-baloch-murdered-by-brother-in-multan-police
7. Express News Service, "Tamil Nadu: Girl commits suicide after morphed pics appear on Facebook," *New Indian Express*, June 29, 2016. [Online]. Available: http://www.newindianexpress.com/states/tamil-nadu/2016/jun/28/Girl-commits-suicideafter-morphed-pics-appear-on-Facebook-885793.html
8. N. Sambasivan et al., "'Privacy is not for me, it's for those rich women': Performative privacy practices on mobile phones by women in South Asia," in *Proc. 14th Symp. Usable Privacy & Security (SOUPS)*, 2018, pp. 127–142.
9. N. Sambasivan et al., "'They don't leave us alone anywhere we go': Gender and digital abuse in South Asia," in *Proc. ACM Computer–Human Interaction (CHI)*, 2019. doi: 10.1145/3290605.3300232.

Nithya Sambasivan received a Ph.D. in information and computer sciences from the University of California, Irvine. She has received several best paper and honorable mention awards from the Symposium on Usable Privacy and Security and the Association for Computing Machinery (ACM) CHI Conference on Human Factors in Computing Systems. She is a member of ACM. Contact her at nithyasamba@google.com.

Nova Ahmed received a Ph.D. from the Georgia Institute of Technology, Atlanta, concentrating on distributed computing and then returned to Bangladesh. She has received best paper awards from the Symposium on Usable Privacy and Security and the Association for Computing Machinery (ACM) CHI Conference on Human Factors in Computing Systems and the New Investigator's Award from Grace Hopper, and she was a Georgia Tech Research and Innovation finalist. She is a Member of the IEEE, ACM, and Organization for Women in Science for the Developing World. Contact her at nova.ahmed@northsouth.edu.

Amna Batool received a master's degree in computer science from the Information Technology University, Lahore, Punjab, Pakistan. She received a Fulbright Scholarship in 2019 and was a gold medalist (for both graduate and undergraduate). She has received best paper awards from the Symposium on Usable Privacy and Security and the Association for Computing Machinery (ACM) CHI Conference on Human Factors in Computing Systems. She is a member of the ACM SIGCHI Student and International Development Innovation Network. Contact her at batool.amna@itu.edu.pk.

Elie Bursztein received a Ph.D. in computer science from the École Normale Supérieure Paris-Saclay, France. He has received several best paper awards, including awards from the IEEE Symposium on Security and Privacy, the WISTP International Conference on Information Security Theory and Practice, the International Association for Cryptologic Research Crypto Conference, the World Wide Web Conference, and the Association for Computing Machinery CHI Conference on Human Factors in Computing Systems. Contact him at elieb@google.com.

Elizabeth Churchill received a Ph.D. in cognitive science from the University of Cambridge, United Kingdom. She is a Distinguished Scientist of the Association for Computing Machinery (ACM) and a member of the ACM CHI Academy, and she has received an honorary D.Sc. from the University of Sussex and an honorary doctorate from the University of Stockholm. In 2016, she also was awarded the Citris-Banatao Institute Athena Award for Women in Technology for her executive leadership. She is a member of ACM, the Ethnographic Praxis in Industry Conference, and the American Anthropological Association. Contact her at churchill@acm.org.

Laura Sanely Gaytán-Lugo received a Ph.D. in information technologies (E-World) from the Universidad de Guadalajara, Mexico. She received a Faculty Teaching Award from the School of Mechanical and Electrical Engineering at the Universidad de Colima, is a member of Mexico's National System of Researchers, and has won best paper awards from the Symposium on Usable Privacy and Security and the Association for Computing Machinery (ACM) CHI Conference on Human Factors in Computing Systems. She is a member of ACM SIGCHI, the Mexican Academy of Computing, and RedLate Mexico. Contact her at laura@ucol.mx.

Tara Matthews received a Ph.D. in computer science (with a major in human–computer interaction) from the University of California, Berkeley. She has received several best paper and honorable mention awards from the Symposium on Usable Privacy and Security and the Association for Computing Machinery (ACM) CHI Conference on Human Factors in Computing Systems, and she has two papers in the top 10 most-cited human–computer interaction journal articles of 2006–2008. She is a member of ACM SIGCHI.

Contact her at taramatthews@gmail.com.

David Nemer received a Ph.D. in informatics (computing, culture, and society) from Indiana University, Bloomington. He received a Faculty Research Award from the College of Communication & Information at the University of Kentucky and a CHI 2018 Diversity Champions Recognition: Emerging Voice, and he was awarded the 2016 Person of the Year in Science and Technology by the Ministry of Science and Technology, Brazil. He is an associate editor of *Journal of Community Informatics* and a review editor of *Tapuya: Latin American Science, Technology and Society*. He is a member of the Society for Social Studies of Science (4S), Association for Computing Machinery (ACM) SIGCHI, and ACM SIGCAS. Contact him at davidnemer@gmail.com.

Kurt Thomas received a Ph.D. in computer science from the University of California, Berkeley. He received the Internet Research Task Force Applied Networking Research Prize and best paper awards from the IEEE Symposium on Security and Privacy, MALWARE, and the Association for Computing Machinery CHI Conference on Human Factors in Computing Systems. Contact him at kurtthomas@google.com.

Sunny Consolvo received a Ph.D. in information science from the University of Washington, Seattle. She has won a Test-of-Time Award from the Association for Computing Machinery SIGMOBILE, three 10-year impact awards from the International Joint Conference on Pervasive and Ubiquitous Computing, an O'Reilly Defender: The People's Champion Award, and several best paper awards. She is on the editorial board of *IEEE Pervasive Computing* magazine, and she is a member of ACM. Contact her at sconsolvo@google.com.

Digital Object Identifier 10.1109/MSEC.2019.2922091