USER PERCEPTIONS OF TRUST AND PRIVACY ON THE INTERNET

BY KRISTEN ROGGEMANN, GALIA NURKO, AND ALEXANDRA TYERS-CHOWDHURY

OCTOBER 2020

DAI

Shaping a more livable world.

CENTER FOR
DIGITAL ACCELERATION

DAI's Center for Digital Acceleration helps our clients integrate digital tools and approaches across their portfolio, especially in emerging markets. We do this by engaging end users, building digital products, and understanding the broader ecosystems that drive the success of technology-based initiatives. Our clients include bilateral and multilateral donors, private sector companies, foundations, and others seeking to drive positive social change across a cross-section of sectors including health, governance, agriculture, education, and economic growth.

The opinions expressed are those of the authors and do not necessarily represent the views of any government or donor agency associated with the content of this paper.

Design: Jennifer Geib, www.jennifergeib.com

CONTENTS

EXECUTIVE SUMMARY

The internet unlocks economic opportunity and access to critical services for populations around the world—including for unserved and underserved communities. However, a digital divide continues to separate those who have access to digital tools and services from those who do not. As efforts to bridge this divide succeed and more people come online, the number, variety, and severity of digital risks is also rising, sowing distrust in the digitally enabled tools and services on which so many of us rely.

Trust underpins digital adoption. Therefore, a decline in trust poses a stark challenge to national governments, international donors, and private companies seeking to promote digital inclusion. If digital distrust erodes confidence to the point where the unconnected or newly connected are deterred from using the internet, the digital divide will grow, and more people will be left behind at the very time our economies are becoming more digitized. Such deterrence effects have a particularly adverse impact on more vulnerable populations in emerging markets, such as women and girls. To fully realize the potential benefits of internet access, we must match our investments in digital infrastructure, digital tools, and digital services with a commensurate investment in digital trust.

To date, most efforts to sustain trust focus on supply-side interventions to mitigate digital risk. A mobile technology company might repair a coding vulnerability that accidentally exposes people's data; an enterprise may require employees to use two-factor authentication to sign in; a social media giant might develop an algorithm to identify disinformation; or a government may configure its email domains with a validation solution such as DMARC to prevent fraud. These UX/UI and back-end interventions to strengthen online security and privacy are important but represent only half the equation. What's missing is the demand side: how *users* understand the challenge before us.

Today, we lack good data on how users themselves perceive privacy and security online and how that shapes their trust of the internet. By interviewing urban youth in Accra, Ghana and Chennai and Delhi, India about this very issue, DAI hopes to advance the conversation beyond supply-side solutions to encompass demand-side insights that deepen our understanding of whether and why users trust, or don't trust, the digital information and platforms they encounter, and what tactics they use to protect themselves online.

If digital distrust erodes confidence to the point where the unconnected or newly connected are deterred from using the internet, the digital divide will grow, and more people will be left behind at the very time our economies are becoming more digitized. Such deterrence effects have a particularly adverse impact on more vulnerable populations in emerging markets, such as women and girls. To fully realize the potential benefits of internet access, we must match our investments in digital infrastructure, digital tools, and digital services with a commensurate investment in digital trust.

Four thematic areas of exploration

While not nationally representative, the qualitative interviews nevertheless yield valuable insights and highlight commonalities worthy of further exploration across four thematic areas: 1) perceptions of privacy and offline influences; 2) trust of online information; 3) tactics to protect privacy and security online; and 4) gender dynamics. We learned that for urban youth respondents in Accra, Chennai, and Delhi:

1 Perceptions of privacy online are significantly conditioned by factors—perceived or real—in the offline environment, particularly factors such as the attitudes of authority figures (including religious leaders), family members, and significant others. Socio-economic, political, and cultural influences will often lead people to create distinct online "identities" to protect their offline reputation.

2 The existence of mis/disinformation is widely known, yet people's perceptions of what is often dubbed "fake news" – and of how much risk it presents to them personally – vary by geography and depend on how well they understand how digital platforms operate.

3 Tactics to protect privacy and security online differ depending on whether users own their smartphone or share it, on whether they are male or female, and on their level of digital literacy. Users might invent codenames for contacts of the opposite sex, for example, or change mobile application settings, or limit the types of information they share on digital platforms.

4 Offline gender gaps and dynamics influence perceptions of security and privacy online, affecting what digital services women can use and how they use them compared to men. All participants voiced concerns about the offline consequences of online behavior, but those perceptions most acutely limit what women do online, which risks exacerbating the online gender gap and leaving female internet users even further behind.

Recommendations

Based on these findings and the existing literature, we offer the following recommendations:

- ✅ The digital development community should adopt a [10th Principle for Digital Development](#) focusing on advancing digital and media literacy for the user.

- ✅ The digital development community should drive coordinated, cross-sector action to develop and adopt universal (but "localizable") digital and media literacy curricula in an open-source, dynamic fashion.

- ✅ Technology companies, especially global platform providers such as Facebook and Google, should guard against assuming that Western norms apply universally by increasing investment in localized design research and robust user testing when developing privacy solutions for global audiences and marginalized groups.

- ✅ The international development community should fund additional research to better understand privacy and security from a user's perspective, taking particular account of women's views, and exploring diverse geographic, socioeconomic, and demographic settings.

- ✅ Regulatory bodies should engage a diverse group of stakeholders from across the public and private sectors, academia, and civil society to develop fair, innovation-friendly, yet protec-tion-focused privacy and security policies that strengthens an open, interoperable, peaceful, inclusive, and secure internet.

In working to increase digital inclusion, focusing on demand-side issues shines new light on how best to maintain trust. We hope our approach informs and provokes further conversations between technologists, international development practitioners, and policy makers, and encourages them to renew their attention to new, veteran, and even unconnected users.

Let's continue the conversation on our Digital@DAI blog and social media channels.
BLOG | TWITTER | PUBLICATIONS | FACEBOOK | LINKEDIN | INSTAGRAM

BACKGROUND AND CONTEXT

Expanding internet access and promoting digital inclusion in "last-mile markets" is a priority for development agencies, national governments, and private companies—and rightly so. The costs to countries that do not offer their populations internet access is high: studies[1] have detailed the internet's macroeconomic boost to GDP, the positive impact of digitization on small business revenue and job creation, and the ways internet access can improve learning and health outcomes or catalyze civic engagement.[2] Over the past 30 years, massive investment in infrastructure has afforded internet access to nearly 54 percent of the global population.[3]

Complementing this investment in access, we need a parallel investment in trust. In its 2013 white paper, *Hierarchy of Cybersecurity Needs,* Microsoft identified trust as a key element of cybersecurity.[4] In 2018, DAI made the case that trust is also a key element of digital inclusion, because distrust deters participation in the digital marketplace.[5] Two related factors that undermine trust are low digital and information literacy, especially if they cause people to feel their privacy or security has been violated. Therefore, it is incumbent on the digital development community to update its understanding of digital inclusion: not only must we expand global internet adoption in a way that is accessible, affordable, relevant, and secure, but we must do so in a way that builds trust, in large part by ensuring that those who use the internet are well versed in the ways of the digital and information marketplace. Focusing on the "demand side," this report seeks to put the user at the center of the critical conversation surrounding internet trust and digital inclusion.

The internet of opportunity also introduces risks

With the increase in internet access has come an increase in digitally enabled bad actors. Manipulating elections, public opinion, cultural debates, and markets, these malefactors have often exploited existing inequalities or social fissures, often amplifying their activities on digital platforms. In some cases, the information shared online results in physical violence. For instance, military personnel in Myanmar used Facebook to incite violence against the country's Rohingya.[6] In the run-up to the 2017 elections in Kenya, fake images circulated widely across social media, creating fear that violence would erupt, potentially leading to destabilizing events around the country.[7] The circulation of false information, whether intended to cause harm or not, creates confusion within a society and can increase distrust not only between communities, but also of the underlying digital platforms themselves. Other forms of digital misbehavior have also been on the rise, including cyber crime, digital surveillance, and online harassment. Each comes with associated offline harms, whether financial, reputational, psychological, cultural, political, or physical.

DIGITAL INCLUSION

DAI defines it as: the expansion of global internet adoption in a way that is not only accessible and affordable, but also relevant, trusted, and utilized by digital and information literate population, who are empowered educated participants in the digital marketplace.

"If people don't trust the internet, no one will use it"

— Male, Delhi, India

Low digital literacy creates a uniquely human dynamic to the challenges of online privacy and trust, one that requires uniquely human-centered interventions. With the recognition that it is much easier and more efficient to train an artificial intelligence system than educate 4.6B individual internet users, there is no magical algorithm that can identify and mitigate all the cyber harms on their platforms, especially given that disinformation and misinformation as well as cyber crime is often uniquely context specific.

These challenges to online information integrity are not limited to low- and middle-income countries. Think of the efforts to compromise the 2016 U.S. Presidential election, the breach of the Marriott hotel reservation system, the UK's Brexit campaign, and the ongoing "infodemic" related to COVID-19. The potential demise of trust in the internet poses a major challenge. In addition to providing access to valuable information and driving economic growth, digital tools facilitate access to critical services such as healthcare, electricity, or banking that increasingly rely on a foundation of a safe, secure, and trusted internet. COVID-19 highlights how essential digital tools and services are to promoting business continuity, ensuring service delivery, sharing critical information, and communicating with loved ones. At the same time, the weaknesses and vulnerabilities of this digital infrastructure are also becoming more evident, as seen through data breaches of popular mobile applications, cyber attacks on global health institutions, or the wave of false or manipulated information about the coronavirus. Although these vulnerabilities are not new, the rapid, global transition to fully virtual business, government, and education, as a result of the global pandemic, has brought them into stark relief.

Is fixing tech with more tech the only solution?

Fixes to security, privacy, and trust challenges are more often than not driven by the supply side of the digital ecosystem. For instance, a technology company might repair the code of a mobile application to patch a vulnerability that accidentally exposes people's data; an enterprise may require employees to use two-factor authentication to sign in, or a government might configure its email domains with a validation solution such as DMARC to prevent fraud. Developers might change the UI/UX of an application or website to improve user-friendliness or employ artificial intelligence (AI) and machine learning to fight off cyber attacks and identify or ring-fence misinformation and disinformation. These supply-side responses to mitigate vulnerabilities are critical to protecting people, businesses, and governments from potential cyber harms.[8] Yet they only solve half of the puzzle.

Supply-side solutions do not address one of the weakest links in the internet ecosystem: people themselves. Research finds that most breaches of information stored on digital tools and services are actually a result of people (users) employing weak or repeated passwords.[9] Nor do supply-side interventions adequately address the cultural norms around identity, privacy, and agency that influence how people interact with digital technology and how they perceive their privacy and security online.

Female users are particularly exposed to the risks and adverse effects of technology (and digital tools and services) since 95 percent of online harassment and negative or aggressive digital behaviors are aimed at women and girls.[10] Female users' (and their families') concerns about cyber safety, their distrust of the internet, and their fears about potential digital harms are acting as a deterrent to internet usage, and women and girls are increasingly reducing or restricting their usage of digital platforms and services as a response[*].

---

* Such as being exposed to inappropriate content, risks to personal safety, online bullying and harassment, compromising of personal information or data, and perceptions that online relationships can damage reputations.

Furthermore, low digital literacy† creates a uniquely human dynamic to the challenges of online privacy and trust, one that requires uniquely human-centered interventions. With the recognition that it is much easier and more efficient to train an artificial intelligence system than educate 4.6B individual internet users, there is no magical algorithm that can identify and mitigate all the cyber harms on their platforms, especially given that disinformation and misinformation as well as cyber crime is often uniquely context specific.

The importance of demand-side solutions

Building people's trust in the digital tools and services they use will not be easy. Research shows that even digital natives, people who "grew up" online, struggle to assess the credibility of information online or even understand basic concepts of digital literacy, such as distinguishing paid advertising from objective journalistic reporting.[11] The implications of this research for non-digital natives—including populations in emerging markets who are newly online and in some cases have minimal formal education—are concerning. If digital distrust erodes confidence to the point where the unconnected or newly connected are deterred from using the internet, the digital divide will grow and more people will be left behind, at the very time our economies are becoming more digitized. Such deterrence effects have a particularly adverse impact on more vulnerable populations in emerging markets, such as women and girls. To fully realize the potential benefits of internet access, we must match our investments in digital infrastructure, digital tools, and digital services with a commensurate investment in building digital trust. This complementary approach is likely to yield a more authentic form of digital inclusion, in which internet users are informed, empowered participants in the digital world, able to make their own educated assessment of how to engage with and what to trust online. Figure 1 illustrates how DAI's Center for Digital Acceleration has been thinking about the issue.
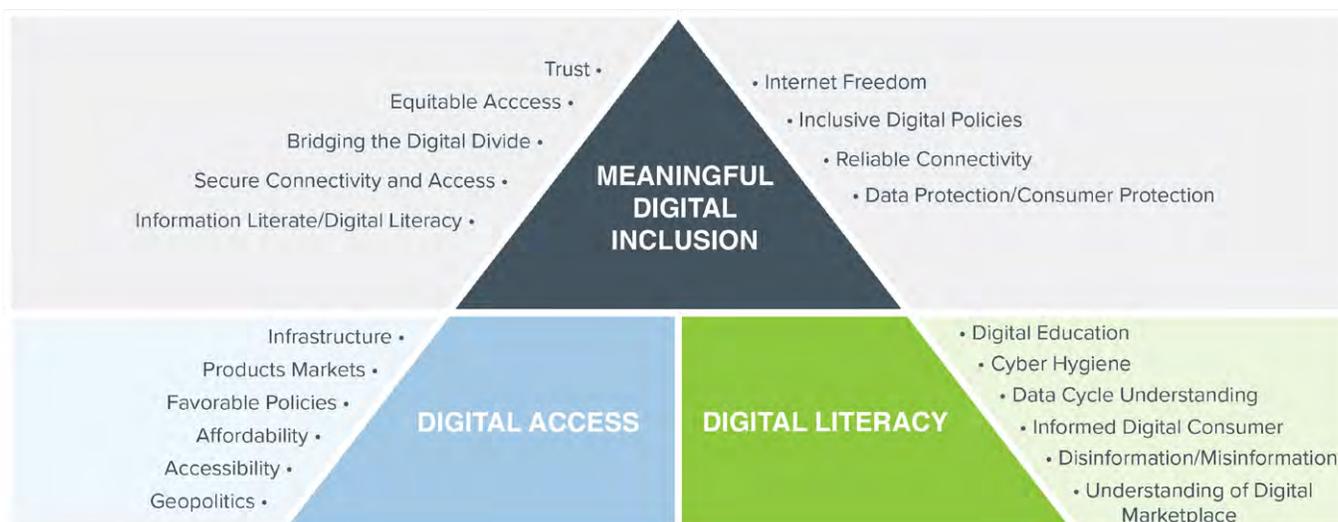
FIGURE 1:
DAI's Center for Digital Acceleration's Cyber Framework.

Turning this framework from concept to reality will not be easy and will require—among other things—de-siloing various communities of practice, including those dedicated to digital development and cybersecurity.

---

† There are multiple active definitions of digital literacy; we are working with the following: the ability to access, manage, understand, integrate, communicate, evaluate, and create information safely and appropriately through digital devices and networked technologies for participation in economic and social life, including competencies that are variously referred to as computer literacy, information and communications technology (ICT) literacy, information literacy, and media literacy.

RESEARCH OVERVIEW AND METHODOLOGY SUMMARY

Purpose of the study

DAI conducted qualitative research among urban youth (ages 18-30) in India and Ghana to find out how users understand their own online privacy and safety and how they trust, or don't trust, the information they engage with via the internet. We chose to focus on young people for two reasons: 1) youth are among the most active user segments on social media and 2) understanding how the high-engagement youth segment parses privacy and trust online is key to designing robust supply-side solutions.

We investigated the tactics young people use to keep themselves and their information private and safe, and discussed their awareness of various aspects of social media and search engine usage, such as personal data tracking and advertising targeting. We also dove into how practices differ when phones are shared rather than individually owned. This research is neither nationally representative nor exhaustive; rather, we hope it will kickstart and inform an overdue conversation about demand-side solutions in support of a trusted internet.

Research objectives

PRIMARY

- Assess internet users' degree of trust and perceptions of privacy and security when they are using the internet and engaging with internet-enabled platforms such as social media

- Assess users' level of knowledge around cyber hygiene, including passwords, phishing, identity theft, and data sharing

- Understand how users perceive the validity of information they consume via the internet and internet-enabled platforms

- Understand what tactics users employ, if any, to protect their privacy and safety online

SECONDARY

- Understand the target population's digital access and use of digital tools

Methodology

Particularly interested in exploring gendered experiences or attitudes, we paid careful attention to gender balance, splitting focus groups by gender as needed and including particular questions designed to explore male and female experiences.

From December 2019 to February 2020, we conducted qualitative research through focus groups with 96 participants in major cities in Ghana and India. The discussions were semi-structured and conversational, conducted in local languages and in neutral venues where respondents felt relaxed, safe, and able to speak freely. Topics covered included device and internet access, usage habits, perceptions regarding the internet, issues of trust and privacy, people's understanding and awareness of trust and privacy— and any tactical measures taken to enhance these attributes—and people's own assessment of their needs. Particularly interested in exploring gendered experiences or attitudes, we paid careful attention to gender balance, splitting focus groups by gender as needed and including particular questions designed to explore male and female experiences.

In Ghana, where urban youth are more likely to own their own smartphones, focus groups were split between users who used the internet regularly (heavy users), and those who used it less regularly (light users). In India, where smartphone sharing (rather than ownership) is more common, particularly for female users, we split the focus groups between users who own their own phone and those who share a phone, based in part on secondary evidence[12] that users who own phones are more likely to have developed digital literacy through increased exposure to the internet. This focus on owned vs. shared in India meant that the groups then needed to be split by socio-economic classification (SEC)[‡], as participants with their own smartphones tended to come from higher SECs, and participants who shared smartphones from middle SECs, as determined by SEC definitions in India and verified by a review of income, education, and material possessions.

[‡]   The Socio-economic Classification grid is a classification of Indian consumers based on parameters such as education levels of the head of the family, and his/her disposable income. This classification was developed by the Market Research Society of India (MRSI) and is followed by all research organizations within India. For this study, respondents were split into SEC A/ B (higher SECs) and SEC C/D (middle SECs). For more details, see https://mruc.net/uploads/posts/b17695616c422ec8d9dadafc1c3eec26.pdf or https://en.wikipedia.org/wiki/SEC_Classification

Participant recruitment and sample

Participants were recruited by partner qualitative research firms in-country.

Ghana

In Ghana, there were 32 participants ages 18 to 30, all from urban Accra, mostly students and workers in diverse fields—artisans, traders, and other professions. Most lived with their parents and siblings; a few were married and lived with their spouses and children.

All participants owned their own phones, almost all of which were internet-enabled smartphones. The most common devices include iPhone (6, 7, and 8) among heavy internet users, and Samsung Galaxy S6 and Galaxy Note among light internet users.

We disaggregated the groups based on:

- gender
- mobile internet access and usage (heavy and light users)[§]

India

In India, there were 64 participants ages 18 to 30, from Delhi and Chennai (urban Tier 1 cities).

We disaggregated the groups by:

- gender
- age (18 to 23, and 24 to 30)
- socio-economic class (SECs A/ B and C/D)
- smartphone access (owned and shared)

Please see Research Methodology for Cybersecurity Frontier Insights: Perceptions of Trust and Privacy on the Internet for a further breakdown of participants and sites, and focus group discussion guides.

[§]   Heavy and light users were defined by their internet usage and spend. Heavy users use mobile internet 6 or 7 days per week, and spend 50 Ghanaian cedis (US$8.70) or more a month on mobile data; light users use mobile internet fewer than 4 days a week, and spend 20 Ghanaian cedis ($3.70) or less a month on mobile data.

RESEARCH FINDINGS

To add context to our research findings, it is important to understand what participants in Accra, Chennai, and Delhi used their internet-enabled mobile phones for. Figure 2 summarizes the purposes to which young people put their phones in these locations.

"How we use our phones."
What participants in Accra, Chennai and Delhi use their phones for.

Participants in Accra use their phones for:

ONLINE ACTIVITIES

- Social media communications
- Research
- Read the news, religious texts, or books
- GPS
- Payment/financial transactions
- Entertainment
- Work

OFFLINE ACTIVITIES

- Calls
- Games
- Pictures
- SMS
- Radio
- Music
- Camera
- Flashlight
- Alarm clock
- Calendar

Participants in Chennai and Delhi use their phones for:

PHONE OWNERS

- Social media communications
- Shopping
- Food/taxi orders
- GPS
- Payments
- Entertainment
- Work

PHONE SHARERS

- Social media communications
- Shopping
- Search
- Entertainment
- Work

FIGURE 2: Mobile phone users in participating in the study use their phones for a variety of offline and online purposes.

PHONE SHARING: BORROWING, LOANING, AND GENDER DYNAMICS

We investigated phone sharing in India and observed a gender difference between respondents who share smartphones. Generally speaking, male sharers tended to loan; female sharers borrowed.

All male phone sharers owned their own basic mobile phones (non-internet enabled), but they either borrowed a smartphone belonging to a parent (for younger respondents), or were the primary owner of their own smartphone and loaned it to their wife or children (for older respondents).

None of the female phone sharers had their own basic mobile phone. Some, however, had their own SIM that they used in a relative's phone. None were the primary owners of a shared smartphone: they borrowed their spouse's or relative's smartphone when the primary owner was not using it.

THEME 1

Participant Perceptions of Privacy and Offline Influences

Participants show a keen understanding that online behavior can have offline consequences; and they modulate their online behavior to mitigate uncomfortable offline experiences

How online behavior affects offline relationships

For urban youth respondents in Ghana and India, their perceptions of privacy were influenced by offline cultural norms. For instance, in Ghana, many respondents felt they had to restrict the type of content they shared on social media because members of their church or mosque community might see the posts and criticize them. This inhibiting effect applied especially to the sharing of images or music that participants thought would be seen as inappropriate either by religious leaders or their community. This constraint was common across all respondents, regardless of gender or internet usage patterns, although female respondents in particular avoided sharing pictures that showed parts of their body that could be seen as inappropriate.

Fear of social censure also meant keeping private affairs hidden from immediate family members or close friends. For one male user, it meant hiding his online betting activity for fear that it might be perceived by his community as indicating a want of money; a female respondent hid her online gambling for fear of social judgment. Other participants cited personal experiences that made them wary of sharing information online, particularly pictures. In one example, a participant shared the cautionary tale that his friend had been fired after being tagged in a picture taken at a party. In another example, a male heavy internet user said he was comfortable sharing information such as his age, but not his location because when he previously shared his location online, someone with whom he had had a misunderstanding tracked him down, which led to a physical altercation.

Female respondents were more likely to feel less in control over their actual phones and their online activity, compared to male respondents, because of monitoring by other people. They occasionally lent their phone to family members (husbands, siblings, or children) or partners (boyfriends), and so were wary of what other people might see. Some female respondents also reported having their social media accounts and activity tracked by their partners, as their partners wanted to be sure that the respondents were

❝ Participant voices

"You cannot show anything to your dad, whether good or bad. Because when you show good things, bad things may pop up. You have all friends and family members sitting there [in the photo]. And that bottle of alcohol is visible....among the [soft] drinks bottle. Then you will explain [to your dad] all [of you] were drinking. Then the question [is] 'with whom did you go?'."

– Male, older, own phone, Delhi

not seeing anyone else. In short, participants show a keen understanding that online behavior can have offline consequences; and they modulate their online behavior to mitigate uncomfortable offline experiences.

In India, perceptions of privacy show some commonalities but differed depending on whether the participants shared their phone. Among all participants there was general resignation and feeling that privacy is "a utopian dream." In the case of phone sharers, privacy meant protecting their social media accounts or contacts from the person they were sharing the phone with (parent, husband, wife, or sibling). For older males in Delhi who shared phones, it also meant limiting any content shared on social media that may indicate their location to a criminal who could use it to plan a robbery against them. For phone sharers in Delhi and Chennai, the prospect of repercussions in the physical world (concerns about a phone being stolen or personal relationships being damaged) outweighed the risks of engaging in the virtual world (such as data theft or exposure to misinformation).

For owners of smartphones, male and female alike, privacy concerns are bound up in concerns over social status and social life. In other words, there is a willingness to sacrifice privacy for the thrill of seeking social validation through likes, comments, or other social media interactions, particularly from friends online. Nevertheless, for both male and female participants, as well as smartphone owners and sharers, there was a consensus that it is important to maintain privacy online from parents or elders, and to a certain extent close friends and cousins, for fear of offline consequences. In contrast, participants felt much more comfortable sharing information online with distant friends or strangers, in the hope there would not be offline consequences.

Participants from both Ghana and India go through a mental exercise to model what the benefits and consequences of engaging online might be. Figure 3 provides an illustrative example of what this mental model might look like based on the research findings.

Among all participants, there was general resignation and feeling that privacy is "a utopian dream."
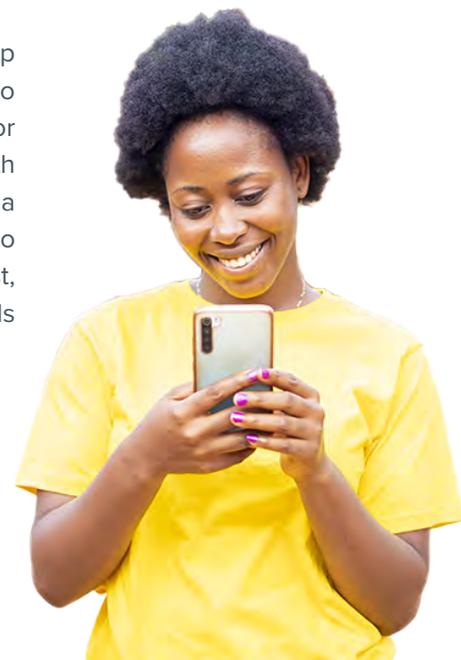
"I can't put a picture of myself and my boyfriend on my display picture [profile picture] because my pastors and church members will question me."

– Female, 18 - 30, heavy internet user, Accra

"Should I...?"

A "mental model" of how participants weigh the consequences and benefits of engaging online.

LEARN OF A NEW APPLICATION

"What value will it add to my life? Social? Professional?"

"Should I download it?"

"What information do I need to share with the application?"

"Who will be able to see what I post?"

"Who recommended it?"

"If I use this, might my parent, sibling, significant other or religious leader find out? What happens if they do?"

"If I don't download it, will I be missing out on something?"

DECISION POINT

FIGURE 3: MENTAL MODEL

When faced with the question of whether to engage with a new application, users go through a complex assessment of the benefits and consequences, considering some or all of these questions in making their decision.

> "They know what we search for... If you search for a product on Amazon, the ads related to that product will come on Instagram and even YouTube. If you search for a phone cover on Amazon, you will get phone cover ads on Instagram. Everything is connected. They are just different platforms, but they are all connected with each other."
>
> Male, younger, shared phone, Chennai

Knowledge of online data sharing

Knowledge of how data is used on the internet differed significantly between Indian and Ghanaian participants. Young men from Chennai who share phones were well aware that Facebook owns a family of mobile applications, including WhatsApp and Instagram, both popular in the country. They also understood that the internet is interconnected, in the sense that if you search for one thing on Amazon you may get advertisements for it on a distinct online service, such as Instagram. Younger male phone owners in Delhi also were aware of cookies, calling them out as a way that internet browsers track their browsing to target ads. Many of them deleted their cookies as a result. The younger male phone sharers in Chennai also were familiar with cookies, though the rest of the participants across Chennai and Delhi did not mention them.

In comparison, participants in Ghana had minimal awareness of the data exchange between platforms for advertising purposes: only three of the participants in Ghana had any awareness of platform and app-level data scraping or sharing. When the facilitator described these features of online services, including how data scraping and monitoring works, most participants in Ghana felt betrayed, insecure, or disappointed. Others felt they were ignorant of this aspect of the digital economy because they had not read the privacy terms and conditions. Those who did know about data scraping and sharing of personal data were male participants who had learned about the issue on the news; they told the facilitator that once they understood the ramifications of data scraping, they "felt scared," an admission of unease that extended to their perception even of well-known brands. Notwithstanding their ignorance of data scraping and sharing practices, male heavy internet users, some male light internet users, and a few female heavy internet users tend to lie about their age or other information a website or application might ask in the account creation process. Many said that sharing such information made them feel vulnerable to the owners of those websites or applications. See box opposite.

TRUST CUES

When it comes to making decisions about what mobile applications to trust, participants in India and especially Ghana rely on word of mouth referrals from friends or family. For Indian participants, trust cues also include the settings or features available on an application, including whether messaging apps offer end-to-end encryption, user-controlled privacy settings, or one-time-passwords as a way to verify their identities. Another determining factor for trust was a reliable connection: poor connectivity experiences with specific applications—payments, for instance—led some participants to switch to applications with more reliable connectivity. Additionally, known brands like Facebook or Google inspired trust among some Indian and Ghanaian participants. In both countries, participants explained that trust may decline as a result of a personal experience or someone in their circle getting hacked or defrauded, including on applications created by trusted brands.

"They [other people] would trust Facebook. They will download many apps like Amazon and Flipkart. We can [have] privacy settings in Facebook; we can use Facebook safely as well."

— Female, older, shared phone, Chennai

DISCUSSION AND ANALYSIS: PARTICIPANT PERCEPTIONS OF PRIVACY AND OFFLINE IMPLICATIONS

For participants in both Ghana and India, concerns about privacy online centered around the ripple effects of how their digital behavior might be interpreted by people in their immediate networks and communities, and how that might lead to offline consequences. Specifically, they feared being judged negatively by those close to them. However, particularly for smartphone owners in India, there was an increase in risk tolerance because obtaining followers or likes on social media is interpreted as improving their social status, even if the people engaging with the online content are not in their immediate offline circle of family, friends, or peers. This is most evident in Figure 4 (opposite).

This understanding of privacy revealed in our discussions with Indian and Ghanaian youth stands in contrast to the way privacy is often conceived in markets such as the United States. For instance, in a recent PEW survey of American adults, a majority of them described privacy by reference to the following themes: "Other people and organizations not being able to access their possessions or private life", "Control over information, possessions, self; deciding what's accessible to others" "Themselves, their personal information and possessions, the desire to keep things to themselves."[13]

For the Americans consulted here, privacy is associated with having control over the information you store online, rather maintaining a certain image offline. Although Indian participants, more so than Ghanaians, were aware that their online information might be exploited, their greater concern was how to ensure privacy from their offline community. In Ghana and India, privacy concerns also tend to be more intimate: keeping online activities secret from other people in the household or personal acquaintances in the community, for example, rather than mitigating cybersecurity risks posed by anonymous online actors. These differences are important because many of the most popular smartphone applications or social media sites are designed by U.S.-based companies that often are most responsive to U.S. consumer understanding and appetites, rather than some of their consumers in low- and middle-income countries.[14] We come back to these findings in our takeaways for stakeholders.

> "Authorized companies such as Google are trusted."
>
> — Female, older, shared phone, Chennai

> "It's a breach of trust because I told [them] to keep it [private], not to share it with others."
>
> — Male, 18 - 30, light internet user, Accra

FIGURE 4:

Shifting online identities

Participants express different identities when online depending on the audience they're engaging with.

DIFFERENT
AUDIENCES →

	FAMILY AND RELATIVES	BEST FRIEND GROUPS	OTHER GROUPS (SCHOOL/COLLEGE/ COLLEAGUES)
Identity expressed online	⫸ RESERVED	⫸ CANDID	⫸ PARTICIPATORY
GHANA: Types of conversations/-content shared	⫸ Pictures ⫸ Carefully curated sensitive information* intended for a specific person ⫸ Certain 'inappropriate content' hidden from relatives or religious leaders	⫸ Carefully curated sensitive information* intended for a specific person	⫸ Advice ⫸ Religious quotations ⫸ Jokes ⫸ Funny videos
INDIA: Types of conversations/-content shared	⫸ Sending morning messages (GIFs and emojis) ⫸ Sending voice messages, in case of call not being received	⫸ Friendly banter ⫸ Random chatting and discussion ⫸ Memes and news	⫸ Pictures that are considered more personal, like from school ⫸ Friendly banter ⫸ Announcements related to personal life or professional achievements

*For further discussion of what participants consider 'sensitive information", see page 27.

> "One time my Facebook account was hacked. Then [my] fear was [if] they....
> post something negative, because our relationship with friends and family
> gets badly impacted. This is one thing. And then there are our banking
> details."
>
> — Female, older, own phone, Delhi.

THEME 2

Trust of Information Online

Both Indian and Ghanaian participants recognize that mis- and disinformation are a growing concern, and many participants had anecdotes and examples of mis/disinformation having an impact on "offline" lives. Despite this growing awareness, internet users in both countries had varying perceptions of their own vulnerabilities to mis/disinformation and expend differing levels of effort in verifying the information they encounter online.

In India, participants across gender, phone ownership status, and age were all strongly aware of the prevalence of fake information on the internet, but they did not feel particularly vulnerable to it unless they themselves had had personal experience with the adverse impact of false information. It was only when respondents had faced backlash from their peers for sharing fake news that they tended to think twice about sharing something. There was also acknowledgment of the time and effort it takes to verify information encountered online, and most participants did not judge that effort worthwhile unless it was clear they were personally affected.

Male participants in Delhi were aware of social and government-led initiatives to counter fake information, including initiatives that potentially increased surveillance. Across participant groups, people employed information literacy and digital literacy-driven tactics to test the veracity of online information. Active steps included checking whether the source of the message is an active number in platforms such as WhatsApp, scrutinizing the content for details that indicate veracity, or verification via search and confirmation. Participants who took active steps to verify information tended to be from a higher socio-economic background than those who did not take such steps. That said, socio-economic status was not a determining factor when it comes to awareness of false information.

DISINFORMATION

Information that is false and deliberately created to harm a person, social group, organization, or country.

MISINFORMATION

Information that is false but not created with the intention of causing harm.[16]

Needless to say, participants did not necessarily use the terminology of disinformation and misinformation, they were more likely to refer to it as false or fake information, or "fake news."

"In today's India wherever [there was] violence, WhatsApp was majorly responsible for it because of the messages that were circulated which led to protest conditions and fights."

— Male, older, shared phone, Delhi

"There is a lot of fake news, like actors have passed away, or fake gossip...we can make out it to be fake due to our experience [with fake news]. I once saw a video saying Aishwarya Rai Bachan has become a widow. Later I searched [online] for it and came to know the truth. Next day I saw [Aishwarya and her husband's] picture in the newspaper, so I realized that it was fake news."

– Younger, female, shared phone, Delhi

"TV3 is trustworthy , you can trust TV3 on their information...every time that you come on social media"

– Male, 18-30, light internet user, Accra

In Ghana, almost all participants had encountered online information they thought was trustworthy but turned out not to be. Many of the participants in Ghana framed their belief or disbelief in information online in terms of its source— Google, Yahoo, Play Store, YouTube, Wikipedia, and Ask.com are all examples of trusted sources believed by participants to operate with strict privacy regulations and to offer genuine, global, and robust platforms. Tech-savvy males (heavy internet users) also cited WhatsApp as a trusted source, generally due to its two-step user verification and encryption. Participants also named specific qualities of trusted SMS and call-based information judged by the way it came to them on their phone (see text box).

Sources known to spread false information were, almost by definition, not trusted, nor were platforms where account hacking is thought to be rife—including Facebook and Instagram. These two platforms in particular are also perceived to be less private. As in India, Ghanaian participants do adopt certain tactics to check the authenticity of information online—perhaps by searching for corroboration on trusted Ghanaian news sites such as TV3 or Joy FM—but again, not every participant will go through these steps.

QUALITIES OF TRUSTED SMS AND CALL-BASED INFORMATION

Content (SMS or calls) from personal contacts base, transactional notifications from MNOs, banks, hospitals and Truecaller are trusted.

They usually use their formats/recognized numbers to determine the authenticity of a service provider.

Truecaller is trusted for revealing the identity of persons whose contact are not in an individual's phone book.

DISCUSSION AND ANALYSIS: TRUST OF INFORMATION ONLINE

The findings from both India and Ghana fall squarely in line with the global trend of escalating mis- and disinformation eroding internet users' trust. User fatigue—the sheer time and effort it takes to validate the truthfulness of information found online—is one of the more pathological consequences of pervasive disinformation. Additionally, while "consider the source" may be one of the foundational precepts of digital literacy, indiscriminately trusting "known brands" such as Google or Ask.com propagates a troubling paradigm that equates "fame" with trustworthiness. We elaborate on these findings in our takeaways for stakeholders.

> "We get forwarded messages that the school or college is closed tomorrow. We would think it is true and forward it. It would look just like our college circular, and says that tomorrow is a holiday or tomorrow there will be cultural programs. They would mostly take the previous year's circular that informed of leave on that particular date, and send it now without even changing the date. People would not look carefully at the year in the date, and would not go to college. But the college would actually be working on that day."
>
> — Male, younger, shared phone, Chennai

THEME 3

Tactics to Protect Privacy and Security Online

In both Ghana and India, tactics to protect privacy and security online include using passwords, employing phone and app locks, limiting who can view posted content by changing certain settings on applications, and limiting the notifications received to avoid the curiosity of prying family members.

Ghanaians were only minimally aware of some of the more complex issues around online security, such as phishing. The most common online security threats noted among participants were hacking, scams, misinformation, identity theft, and fake news, but they knew little about these threats, and the general view—held by both men and women—is that social media "show-offs," celebrities, and politicians are the people prone to privacy and security violations.

One area where participants did have significant knowledge is phone-based scams, especially with regard to mobile money. Ghanaian mobile network operators have aggressively championed education around such scams, and thus most people are able to protect themselves. Most participants used settings on applications and their phones to protect their security and privacy online. For most participants, this meant having passwords on their phones or for specific apps and changing the settings of people who can view their social media posts. A few participants used virtual private networks, though less to protect their privacy or security than to view content blocked to Ghanaian IP addresses.

WHAT INFORMATION IS CONSIDERED SENSITIVE

In our focus groups in Ghana, respondents indicated they considered the following sensitive information: location, videos of family/friends, relationship details, nude pictures, secret conversations with family/friends, business details, gossip, age, personal address, health issues, financial details.

In our focus groups in India, respondents indicated they considered the following sensitive information: financial information, personal matters (like family dynamic), passwords. Respondents also discussed sensitive information available on platforms, for instance, extremist messaging, or nude images shared online that a social media platform might signal is sensitive. Phone sharers were more conscious about not sharing sensitive information and in general the feeling of vulnerability was much more acute amongst shared phone users.

> "I remember a friend of mine, somebody hacked his account and was asking people for money. As for me, I wouldn't know what to do if somebody hacked my account"
>
> — Female, 18-30, heavy internet user, Accra

Some participants in Ghana reported understanding that there are privacy and security risks to engaging online, but felt they had inadequate information for how to address those risks effectively.

Independent of application settings, choosing what information to share was another offline protection tactic cited by Ghanaian participants, especially women. Both male and female participants believe females are more vulnerable online due to low digital literacy skills. Among the steps they reported taking: not posting images of themselves; limiting who can view those images; refusing to share financial information online; not posting sensitive content on a public profile, but instead sharing it through private channels, such as WhatsApp or Facebook Messenger, deemed to be shared only between sender and recipient. As an extra layer of precaution, some participants also delete the messages after sharing to ensure privacy, especially when they feel the information is sensitive (financial information, for example).

Many participants discussed the internal conflicts involved in engaging in the digital marketplace, in the sense that some valuable applications, such as WhatsApp or Facebook, might require you to share a phone number or email, even when you are uncomfortable doing so. In addition, some participants reported understanding that there are privacy and security risks to engaging online, but felt they had inadequate information for how to address those risks effectively. Some female participants even resorted to prayer in the hopes of warding off hacking or other privacy violations. Finally, participants feel strongly that both private and public players have a responsibility to champion the education and protection of internet users. Specifically, participants felt that Ghana's Ministry of Information and Data Protection Agency were both well-positioned to develop strict privacy and security policies, and educational institutions were identified as key drivers of digital literacy programming.

Indian respondents were more aware of security and privacy risks online, including methods to mitigate those risks effectively. At the same time, there were key differences between those who own their phones and those who share a phone. Users who owned their own phones employed a variety of safety and privacy managing behaviors such as using the phone password or fingerprint lock as well as individual app locks to be doubly safe. Female respondents in particular took extra precautions, such as using dummy folders with passwords, setting up pre-designed secured folders, and keeping location details hidden when online. Younger participants employed tactics such as using a restricted view on WhatsApp to shield their chats. Higher socio-economic status participants and men also employed incognito or private mode while browsing, suggesting that these segments had higher awareness of the built-in advanced privacy features offered by individual applications.

"**Some people know my screen lock pattern, [but] even if they are able to access the phone, they will not be able to access the apps. There is another lock for that. [I use it] mainly to hide these things from friends and colleagues.**"

— Male, older, own phone, Chennai

Shared phone users employ additional protection tactics

Shared phone users take extra precautions to protect their privacy from phone owners, as seen in Figure 5 (below). Phone sharers who share a smartphone but have access to a feature phone tend to use the feature phone's SMS more frequently than other messaging platforms, providing them privacy from the individual they share their phone with, despite missing the advanced functionality of a smartphone. If they are using the messaging apps available on smartphones, they typically either erase their conversations after the fact or log out of the messaging application to ensure privacy. Many of the respondents also clear their search and location histories to prevent a phone owner from looking through them.

Other sharers use more elaborate privacy techniques: saving contacts under a different name (often of the same gender to prevent parents being suspicious), using archiving techniques to hide message threads from non-techie elders, or using dummy apps such as fake calculators to hide personal pictures and videos. Gender differences among shared phone users were especially interesting. Females faced high scrutiny of their phone and internet use by others (particularly male relatives), whereas males had low scrutiny—a discrepancy possibly related to the fact that none of the female respondents who shared smartphones were the primary owners, unlike their male counterparts. Female users were also extremely mindful of their digital footprint, both on the device (the phone) itself and on the internet, whereas males were less mindful of their digital footprint unless it involved a romantic angle that required privacy.

OWN PHONE USERS

Icognito mode or Private mode browsing	Use phone password or fingerprint lock
Not just screen locks but also app locks	Restrict view on WhatsApp
Dummy folders with pass-words, pre-designed secured folders	Not sharing OTP with telecallers

SHARED PHONE USERS

Use SMS more on basic personal phone to maintain privacy but miss the advanced functionality of a smart phone	Delete WhatsApp chats or consciously log out of the personal messenger to ensure privacy
Use archiving to ensure messages are not on top of scrolling menu but are far down or appear hidden so not easily discovered by non-techie elders	Save contacts under a different name. Keep name as same gender as self.
Clear history or location details sharing from Google Maps	Use dummy apps such as Smart Hide Calculator to hide pictures or video

FIGURE 5: COMPARATIVE STRATEGIES
Participants with their own phones have slightly different strategies and behaviors to manage safety and privacy online than those who share phones with other users.

> "Earlier I wanted to [create] online videos, but not [anymore] because my location will be known or shared. Then relatives would know. [My] location [can also be] shared on Facebook....even on WhatsApp there is a location feature, so you have to be very careful. We keep [our] location off."
>
> – Female, older, own phone, Delhi

Both phone sharers and owners were aware of the importance of complex alphanumeric passwords to enhance one's online security, though many acknowledged that reusing one password is simpler than remembering or changing many. In some cases, they stored these passwords in dummy folders to keep track of them. Additionally, both owners and sharers make conscious decisions about what they share online in an intentional effort to keep their online and offline lives separate.

Sense of Control Online

When participants were asked whether they felt control over their online activities, respondents in Ghana mostly said yes, because they can control what they post or what they comment on. Other Ghanaian respondents said they felt control over their phones because they always know where they are. In contrast, respondents in India, both those who own and those who share phones, did not feel they had control over their online activities. Specifically, they cited lack of control over how the data you share online can be manipulated or stolen to create new identities. Furthermore, participants in India view control in terms of the settings they can adjust on the phone or applications, such as changing who can view shared content.

DISCUSSION AND ANALYSIS:
TACTICS TO PROTECT PRIVACY AND SECURITY

In both India and Ghana, privacy was often seen as protection from offline communities. Participants utilized a variety of tactics to protect their privacy and security, both from prying elders and from the growing phenomena of hacking and other online threats. Ghanaians, in particular, want public authorities to take a more active stance in ensuring online security. In both settings, the particular vulnerability of women stood out (gender dynamics are discussed in more detail below). An important difference between the two research settings, worthy of exploration in other markets, is the difference in feelings of control between the urban youth interviewed in Ghana and those interviewed in India. Were these distinctions a result of different levels of digital literacy? We return to these findings in our takeaways for stakeholders.

"Google Maps - there will be history. If we switch it off, nobody will know where we are going. Otherwise the history will be saved wherever we go. We can go [into Google Maps] and delete history...it feels like somebody is watching us all the time. If the [Google Maps location feature] is on it will save the places that you go, but if you switch it off, it won't be seen."

– Male, older, shared phone, Delhi

"I was chatting with my friend on WhatsApp in my phone and my father came and took the phone and I started shivering [worrying]. Then my father gave the phone to my brother and asked to find out who [my friend] is. Then my brother quickly changed the name and saved it as a girl's name and gave it to my father."

— Female, younger, shared phone, Delhi

"Because of archiving, the messages get hidden but if the person is talented and if they want to search for the messages, then they would search [and find them]. And we just go and read it but our mothers just look at phone calls [call logs]."

— Female, younger, shared phone, Delhi
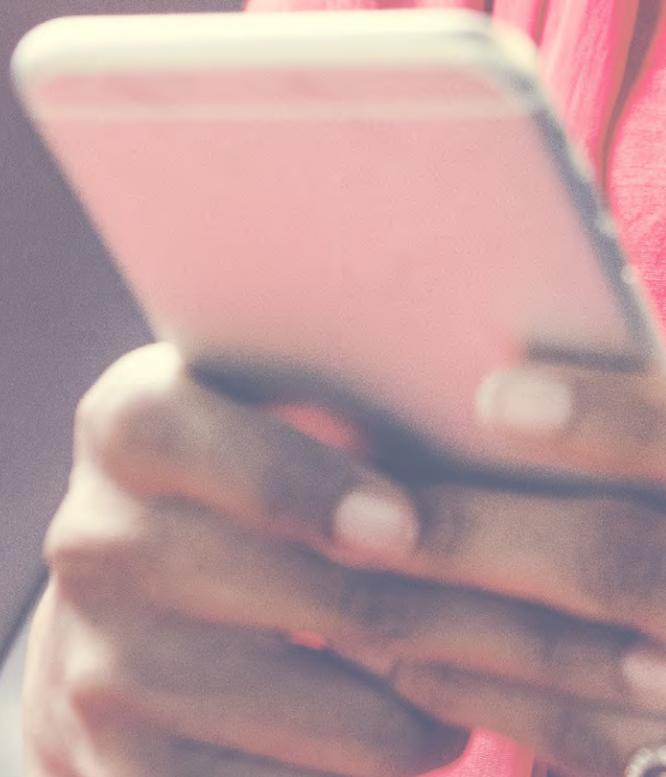
THEME 4

Gender Dynamics

The social dimensions of gender dynamics carry over into digital norms and behaviors, both in terms of how families and communities control a woman's access to and usage of the internet and in terms of how women themselves modify their digital behaviors and utilize tactics that maximize privacy so as not to be seen violating society's gender expectations.

The social dimensions of gender dynamics carry over into digital norms and behaviors, both in terms of how families and communities control a woman's access to and usage of the internet and in terms of how women themselves modify their digital behaviors and utilize tactics that maximize privacy so as not to be seen violating society's gender expectations.

This guardedness is especially acute for females who face more stringent social restrictions. Our research in India found that the very act of going online on social media for certain people would be violating the trust of a family member and/ or partner. Male and female respondents, in both countries, mentioned social expectations that female users should abide by the reigning standards of how a woman should and should not behave (both online and offline), which include not expressing themselves too freely online, or sharing too many pictures. Often, female users—especially younger women— were perceived as vulnerable and in need of protection from the wider world.

Community-moderated dimensions of privacy and trust

Women in both India and Ghana find their access to the internet controlled or moderated in various ways by their communities. They might find their ability to download certain apps or have private logins to social media is curtailed. Or they might find their online behavior is monitored by family.

While this type of community monitoring was felt by both genders, the surveillance of women tended to be more acutely felt by female respondents in both countries. In Ghana, male respondents all reported that they had personally created their own Facebook accounts, whereas more than half of the female respondents (especially those who used the internet less frequently) had had their accounts created by other people (often male and family members or friends, such as brothers, friends, or ICT teachers). Those third parties were able to log into the female users' accounts if they so choose.

"We should not keep our pictures as our display picture [profile picture]. Don't add too many people. Won't update status. Use privacy settings."

— Female, older, shared phone, Chennai

In India, younger female shared phone users reported that passwords used on the shared phone were often used by their brothers to restrict their access to the phone, monitor how much they were using it, and scrutinize what they were doing. For example, brothers would regularly change the password without informing their sisters, making sure that their sisters would need to ask for the password in order to access the phone. This gatekeeping is a good example of how the wider gender digital divide in India undermines user trust and privacy: male shared phone users did not report any community monitoring of this type, as they were mostly the primary phone owners themselves who lent their devices to other people, whereas none of the female users were the primary owners of a shared smartphone, and so were subject to more control and monitoring.

Monitoring of online behavior

Both in India and Ghana, female participants in particular highlighted how much the expectations of female behavior—from their parents, extended family, and the community— intentionally or unintentionally shaped their experience of the internet.

As noted above, the fear of being "found out" in their online lives—in romantic online chats, selfies, photos featuring alcohol or parties, or even simply *having* a Facebook account—drives participants to constantly restrict and adjust their social media and internet experience to maximize privacy and minimize risk of exposure. While both genders are vigilant, female users (especially in India) tend to be more cautious and pragmatic in the online world, in what they share online, and what they delete or keep on their devices, and they take more steps to minimize their online footprint. Not surprisingly, this fear-based behavior was especially pronounced in females who share smartphones.

Female participants in India also tended to be more concerned about their personal life and personal photos falling into the "wrong hands," having their photos maliciously edited or published by strangers, and being "exposed" before their families or offline communities.

All of these concerns often resulted in female users taking measures either to prevent these things happening or reducing their internet usage.
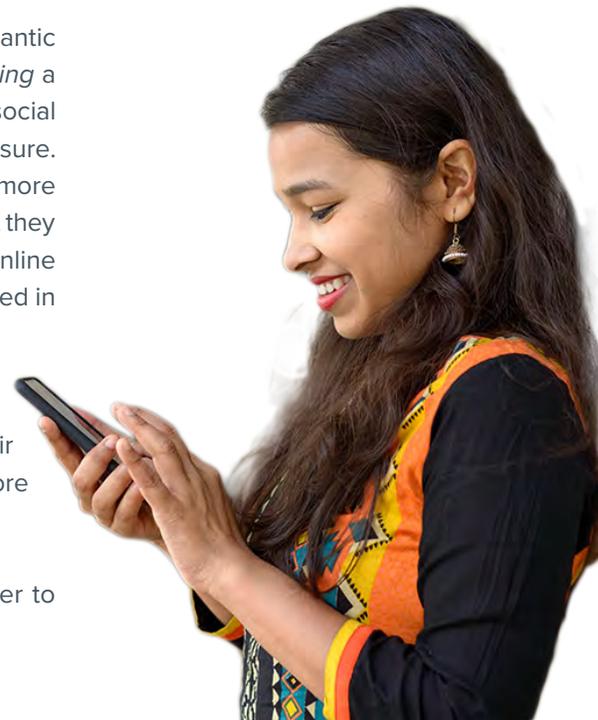
"My picture was Photoshopped by a guy on Facebook. He tagged his photo along with me. One of my friends, who was a mutual friend, texted me to ask whether I know him and I said no. Then he shared the photo with me which was posted online by that guy and the guy had kept it as his profile picture. We reported him on Facebook, took his phone number from his friend and then scolded him and told him to delete all those photographs…"

— Female, older, own phone, Delhi

Self-moderated dimensions of privacy and trust

In Ghana and India, gendered concerns about privacy and trust meant that female users tended to modify their own digital behaviors to protect themselves and maintain privacy in ways that were much more pronounced than those employed by male users. These tactics and behaviors include those in Figure 6 below.

"How can I stay safe online?"

Tactics and behaviors female participants employ to protect themselves and maintain privacy online.

Regularly deleting their activity from their phone and their online browsers, including the history cache, previous chats, and posts—especially among Indian women who share smartphones.

Logging out of social media accounts on shared phones.

Changing notification settings on WhatsApp or other chat or social media accounts, so that incoming messages do not have a notification sound. Female users in Ghana do this so that their family or boyfriends do not read their messages if they hear the sound while the female user is away from her phone.

Saving contacts under a different name and making sure any male names are saved as female names, to remove suspicion if anyone checks their phone.

Creating multiple online identities, often curated for family approval. Female respondents in India, especially younger respondents, reported having multiple accounts on Facebook, Instagram, and WhatsApp.

Moderating and minimizing what they do publicly online—such as not sharing or liking posts, and not accepting friend requests from strangers.

Switching to SMS to chat with boyfriends or friends. Older relatives often do not think to check a phone's SMS history, because chatting via SMS is less common. In India, shared phone users intentionally sacrificed the quality of their user experience by using lower-tech solutions such as SMS in exchange for more privacy and freedom from family members policing their app usage.

Reducing their personal markers online so that they cannot be easily identified. For example, having no display pictures, not updating their status regularly on social media, and using high privacy settings where possible.

Switching to platforms such as WhatsApp, rather than Facebook or Instagram. For many female users in our study, WhatsApp was seen as a safe haven, leaving them less "exposed." WhatsApp is also seen as subject to less scrutiny and disapproval than other platforms, and as more secure because of its end-to-end encryption. In India, particularly, it is popular among female users because it is widely used and therefore familiar, and generally seen as more private than Facebook or Instagram.

FIGURE 6: Tactics and behaviours for staying safe online.

> **"Once my Facebook account was hacked, I couldn't use the account anymore, so the only thing I could do was to open a new one."**
>
> Female, 18-30, heavy internet user, Accra

(Perceived) higher levels of vulnerability

Generally speaking, female users tended to have lower levels of digital literacy than the male users, and the lower the level of digital literacy (which often corresponded to lower levels of internet usage and lower SEC), the less aware of the harms and therefore the more vulnerable the female user was, despite many taking specific precautions to protect their digital privacy,. Female users—especially those from lower SECs, and those who shared phones and used the internet less regularly—often reported not knowing what to do when faced with a digital harm, or what measures they could take to protect themselves.

This was as much about *perceptions* of female users and their digital skills and awareness as it was about their *actual* skills and awareness. Male and female respondents in both countries opined that female users had lower levels of understanding and awareness of the internet and potential digital harms. Male and female participants also raised concerns around trust, security, and privacy on behalf of female family and friends who use of social media. Women in general were perceived to know less about cybersecurity, be more vulnerable, and thus to need "protection"—regardless of whether they actually did have less knowledge or not.

This internalization of social gender norms about what women can and cannot (and should and should not) do online perpetuates female users' beliefs (and those of their families and communities) that they are less capable, more vulnerable, and therefore need to be monitored when online, which further risks widening the gender digital divide. If female users are restricting the way they use the internet and digital platforms because they are fearful of the risks and distrustful of the internet, they will be left even further behind.

Women in general were perceived to know less about cybersecurity, be more vulnerable, and thus to need "protection"—regardless of whether they actually did have less knowledge or not.

DISCUSSION AND ANALYSIS: GENDER DYNAMICS

In both India and Ghana, gender norms have a much greater impact on female respondents' use (and perceptions) of the internet than on male respondents'—which in turn colors females' perceptions of privacy and trust. Female respondents in both countries spoke of having less control and being subject to more monitoring from their community (both in terms of access to devices and the internet, and once they are online). And they are often seen as more vulnerable and less digitally literate. This combination of factors has resulted in fear-based behavior and moderation in online experiences (self-moderated or otherwise), and female respondents using specific tactics and modifying their own digital behaviors to protect themselves and their privacy and online security. These findings regarding the gendered risks of digital technology and the wider gender digital divide, especially in digital literacy, support those of other studies in the same markets[15] and highlight how essential it is to understand female audience segments in different markets, and female user perspectives. They are highlighted in our takeaways for stakeholders.

> "Women are more vulnerable because when they show even some nudity, you will see the way it will go viral....and [women] don't know tech like men"
>
> Male, 18-30, heavy internet user, Accra

TAKEAWAYS FOR STAKEHOLDERS

Internet users are learning to cope with digital vulnerabilities. As digital access expands and awareness of digital risks increases, people are delineating workable boundaries between their online engagements and offline lives, even though the lines are increasingly blurred. Insights into internet users' understanding of these boundaries—including the tactics they use to protect their privacy, identify trusted information or platforms, and assure their security—will be vital to anyone seeking to mitigate digital risks and nurture digital trust.

The following are our key takeaways for technologists, international development actors, and policy makers.
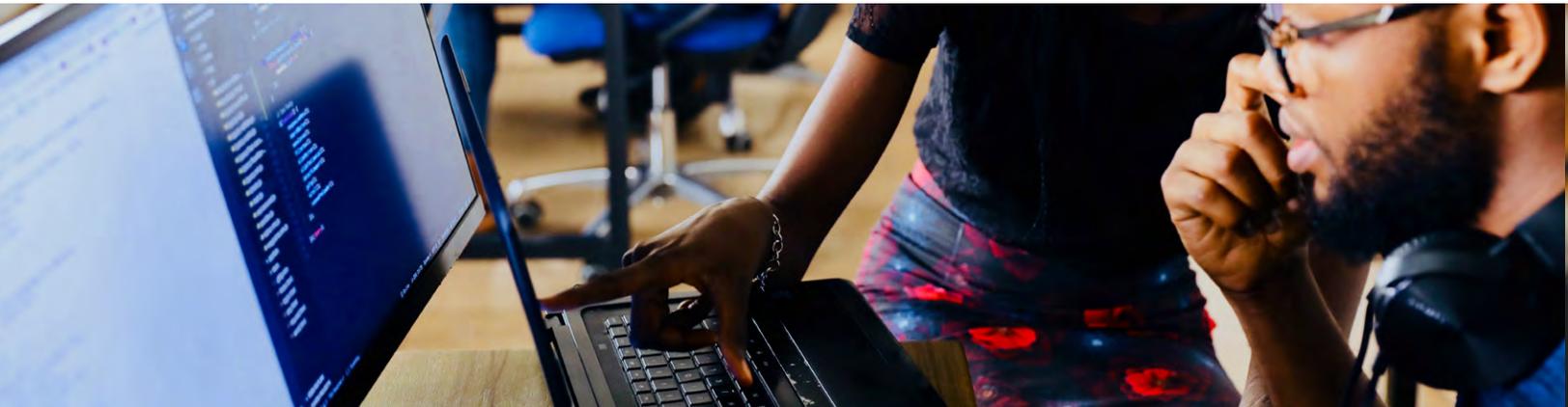
Takeaways for Technologists

Conduct robust, localized user-centric consumer research

☑ In developing products and services, don't assume users in emerging markets will follow U.S. or Western norms, either in mundane matters such as the visual cues to which they respond or higher-order issues such as their mental model of privacy. For example, a floppy disk icon may mean "save" to a Western user who remembers the technology but to more recent users, it does not make sense in the same way.

☑ Investigate how varying socio-economic, cultural, political, or religious backgrounds will affect how users engage with your digital service. How do women and girls' experiences of online services differ from those of men and boys? Do users own their own phones and/or share their devices? How does this affect how they use services? What mental models do people go through when deciding how to engage online? What factors do people consider before downloading an application, sharing a picture, or forwarding a message?

Design features to respond to these local realities

☑ Design for a female as well as a male experience, especially when it comes to ensuring privacy and building trust based on findings from localized, user centric consumer research.

☑ Create more readily understandable privacy and security policies, in local languages, so that people feel and *are* informed when they decide to share certain information through your service.
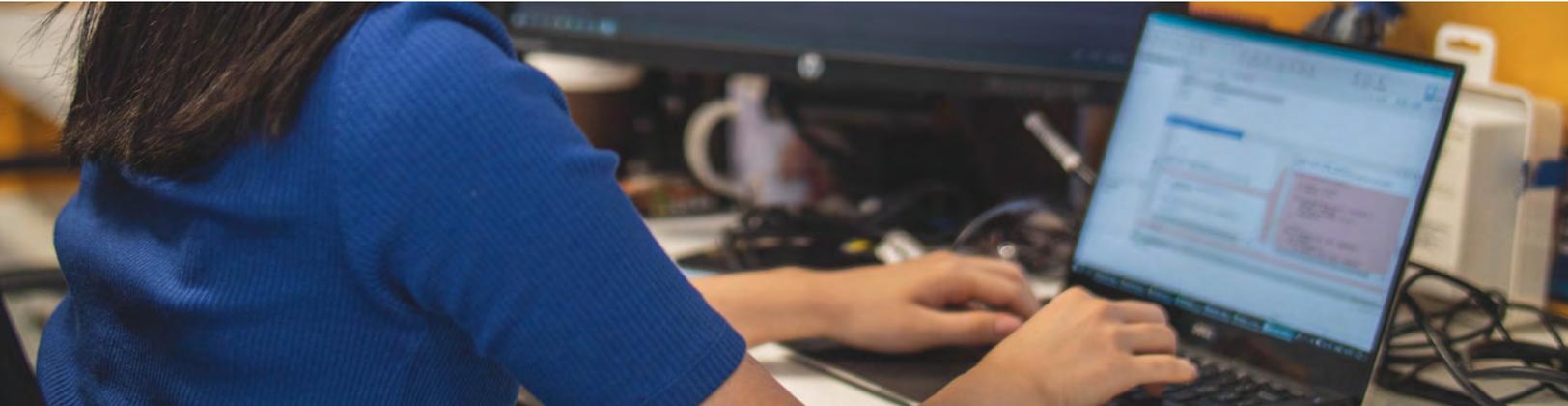
☑ Consider adding features that:

- Ease the burden of creating secure digital profiles. For example, recommending password managers or One Time Passwords; hard coding the number the SMS might come from so the user knows it is genuine.

- Enable consumers in lower- and middle-income countries to wipe or lock their online accounts from unknown or untrusted users.

- Make it easy for users to replicate structures and distinctions in their offline lives—such as family vs. friend circles—in their online profiles.

- Require explicit user permission when sharing what might be considered sensitive information in a given culture. For example, a pop-up box asking "Are you sure you want to post this?"

- Understanding local language nuances and relevant political and historical contexts is important for creating effective labels that highlight misleading information. Technology designers should provide clear, easy-to-read markers that are understandable for even novice users, remembering that users in emerging markets may not respond to the same visual cues as Western users.

☑ Technologists employing algorithms to identify misinformation and disinformation would benefit by building in opportunities for users in emerging markets to provide feedback on these algorithms. Making the machine learning datasets more inclusive and transparent to users will make them more effective.

- Engaging more local staff, people who understand cultural nuances, will help technologists design better tools for local markets.

Explore public-private partnerships to increase digital and information literacy

☑ Consider partnering with public sector actors to improve digital and information literacy for women and girls, particularly in public education systems and other high-touch environments.

☑ Remember the power of corporate advertising to support positive behavior change—consider using marketing channels to promote good online security practice and show the benefits of safe online access, especially for women and girls.

Takeaways for International Development Practitioners

Research user privacy and trust in digital tools, focusing on marginalized groups

☑ Deepen understanding of the relationship between online behavior and offline influences.

☑ Research the needs of women, girls, and marginalized groups (such as the elderly, rural people, persons with disabilities, and ethnic or religious minorities) in various markets, and what privacy and a trusted internet means to them in their context. Pay attention to segments within a population, as none of these marginalized groups are homogeneous and most will intersect to some extent with other groups.

Increase investment in digital literacy programming

☑ Ensure this programming includes instruction in cyber hygiene techniques, so that users of digital tools or services better understand the online ecosystem, enabling them to better protect their privacy and private information.

☑ Ensure all digital programming accounts for socio-economic, cultural, or political factors that may condition users' digital trust or shape their digital behavior.

☑ Tailor programming for women and girls, as well as male and family gatekeepers who may restrict women and girls' access to and use of digital tools and services because of the perceived risks to their wives, daughters, or sisters. If gatekeepers are aware of potential digital harms but also how to mitigate them, this may help tackle negative perceptions of the gendered risks of technology.

Invest in information literacy campaigns

☑   Implement campaigns to educate users about how to judge the veracity of information they find online, and how mis- and disinformation can be spread via the internet.

☑   Ensure that funding for adjacent sectors such as education, technology, and governance includes appropriate targets on digital and information literacy and proactive public policy.

Build partnerships to support a more digitally literate workforce

☑   Consider working with the private sector, formal and informal education networks, and civil society organizations to reach veteran, new, and non-users of digital tools.

Update internal policies and activities to strengthen digital privacy

☑   Hire more local staff who understand the local digital ecosystem, the popular tools at play, common digital risks, and gaps in digital or information literacy across population segments.

☑   Understand the legal environment in which a digital tool or service may be used. In particular, note how privacy or security may be defined differently than in the Western context and respond accordingly.

☑   Develop (or adapt) internal digital safeguarding policies, processes, and practices that focus on women and girls and the gendered risks of technology and apply to any internal program that has digital components.

☑   Support, invest in, and share insights on digital tools and services that consider the female user experience and needs with regards to trust, privacy and security, or that are specifically designed to overcome gendered risks of technology.

Takeaways for Policy Makers

Create a pro-privacy yet innovation-friendly policy and regulatory environment

☑ Work toward robust yet flexible privacy regulations and a dynamic regulatory environment that balances innovation with consumer protection.

☑ Ensure technology legislation is technology neutral and that its rules are applied consistently to all players in the internet ecosystem, supporting a consistent user experience of supply-side privacy and security.

☑ Establish clear cybersecurity laws, privacy policies, and technology regulations that have considered the needs of female users and marginalized groups.

☑ Ensure education policy integrates digital and information literacy as a crosscutting objective with targets for equal participation of men and women.

☑ Encourage technology companies and other digital actors to explain in simplified terms and in local languages their privacy and security policies.

☑ Develop policies that encourage local technology companies to thrive and break into local markets.

☑ To ensure any government-led policy to combat misinformation and disinformation does not inadvertently infringe on people's rights (freedom of expression and so forth), establish an advisory or working group of civil society leaders, academics, private sector representatives, and users to advise policy formulation.

☑ Encourage and enable an independent media.

Engage with diverse stakeholders to strengthen policy making

☑ Engage civil society leaders, academics, private sector representatives, and users to advise on cyber-security policy, particularly focusing on the needs of female users and marginalized groups.

☑ Work with technology companies and other digital marketplace actors to establish a framework for transparent information sharing on data breaches or decision-making by algorithms.

Mainstream digital literacy in educational settings

☑ Mainstream dynamic digital literacy training in school curricula, lifelong learning programs, and informal learning environments, aiming for a universal baseline understanding of cyber hygiene and privacy protection practices online.

☑ Focus in particular on reaching girls and women and ensuring the curricula covers the gendered benefits of technology, along with its risks and potential recourse mechanisms.

☑ Pay particular attention to increasing girls' uptake of STEM subjects (science, technology, engineering, and mathematics) to support more equal participation in the creation of digital tools, as well as increase their confidence and fluency in technology as a consumer.

DIGITAL LITERACY RESOURCES

Digital literacy initiatives have access to a wealth of high-quality materials that can be reused, repurposed, or adapted, rather than created from scratch. Some suggested resources include:

The Chayn Do-It-Yourself Online Safety Guide offers practical advice on how to mitigate risks when online—for example, setting passwords, using secure browsers, and staying safe on social media. It is available in multiple languages.

The GSMA Mobile Internet Skills Training Toolkit, available in multiple languages, has been designed for mobile-first contexts, and it includes a section on security and privacy, and online risks.

The Safe Sisters toolkit is designed for women and girls in Sub-Saharan Africa. It aims to simplify digital security issues, make them relevant to real users, and encourage users to take online safety into their own hands.

Mozilla's Women and Web Literacy has a variety of digital literacy resources, including Teaching Kits on cyber violence, sexting, hacking, and online abuse. While the resources are primarily focused on women and girls, they can be adapted for different audiences.

OUR
RECOMMENDATIONS

Where do we go from here?

To fully realize the benefits of internet access, investments in infrastructure and technology must be matched by a commensurate investment in user trust. This investment can take many forms—from enabling a richer understanding of the demand-side dynamics of internet trust to scaling digital and media literacy education initiatives and cultivating a regulatory environment that balances user protection with innovation.

We hope that with the benefit of our participants' experiences and insights—plus the recommendations and suggestions for further research we have made— technologists, international development actors, and policy makers will be better equipped to navigate the demand-side challenges of establishing digital trust and protecting online privacy. And we hope they are inspired to delve deeper than the scope of this study would allow us to go. Below we suggest some next steps the international technology community can take to realize immediate impact in support of a trusted internet

1 The digital development community should adopt a 10th Principle for Digital Development focusing on advancing digital and media literacy for the user.

2 The digital development community should drive coordinated, cross-sector action to develop and adopt universal – but "localizable" – digital and media literacy curricula in an open-source, dynamic fashion.

3 Technology companies, especially global platform providers such as Facebook and Google, should guard against assuming that Western norms apply universally by increasing investment in localized design research and robust user testing when developing privacy solutions for global audiences and marginalized groups.

4 The international development community should fund additional research to better understand privacy and security from a user's perspective, taking particular account of women's views, and exploring diverse geographic, socioeconomic, and demographic settings.

5 Regulatory bodies should engage a diverse group of stakeholders from across the public and private sectors, academia, and civil society to develop fair, innovation-friendly, yet protection-focused privacy and security policies that promote an open, interoperable, inclusive, and secure internet.

Let's continue the conversation on our Digital@DAI blog and social media channels.
BLOG | TWITTER | PUBLICATIONS | FACEBOOK | LINKEDIN | INSTAGRAM

REFERENCES

1   World Bank. "World Development Report 2016: Digital Dividends." 2016. Accessed July 2020: https://www.worldbank.org/en/publication/wdr2016

2   Deloitte. "Value of connectivity: Economic and social benefits of expanding internet access." 2014. Accessed July 2020: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/TechnologyMediaCommunications/2014_uk_tmt_value_of_connectivity_deloitte_ireland.pdf

3   ITU Statistics. Accessed July 2020: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

4   Microsoft & Oxford Analytica. "Hierarchy of cybersecurity needs: Developing national priorities in a connected world." 2013. Accessed July 2020: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmca

5   DAI. "Digital Inclusion and a Trusted Internet." 2018. Accessed June 2020: https://www.dai.com/cda-cybersecurity.pdf

6   New York Times. "A Genocide Incited on Facebook, With Posts From Myanmar's Military." 15 October 2018. Accessed June 2020 https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html?auth=login-email&login=email

7   Forbes. "Kenya's Election Proves Fake News Is A Serious Threat To International Security." 14 August 2017. Accessed June 2020 https://www.forbes.com/sites/tarunwadhwa/2017/08/14/kenyas-election-proves-fake-news-is-a-serious-threat-to-international-security/#1bcc0cf8491d

8   "The damaging consequences resulting from cyber events, which can originate from malicious, accidental or natural phenomena, manifesting itself within or outside of the Internet." From Ignatuschtschenko, E; Roberts, T. and Cornish, P.N. "Cyber Harm: Concepts, Taxonomy and Measurement" in *SSRN Electronic Journal* · January 2016. Accessed June 2020: https://www.researchgate.net/profile/Paul_Cornish2/publication/315459761_Cyber_Harm_Concepts_Taxonomy_and_Measurement/links/5a97d8f9aca27214056bd63f/Cyber-Harm-Concepts-Taxonomy-and-Measurement.pdf

9   Verizon. "Verizon's 2016 Data Breach Investigations Report finds cyber criminals are exploiting human nature." April 27 2016. Accessed June 2020: https://www.prnewswire.com/news-releases/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human-nature-300258134.html

10   Association for Progressive Communications (APC). "MDG3: Take Back the Tech! to end violence against women." Accessed June 2020: https://www.apc.org/en/project/mdg3-take-back-tech-end-violence-against-women

11   Stanford Graduate School of Education: Research Stories. "Stanford researchers find students have trouble judging the credibility of information online." 22 November 2016. Accessed June 2020: https://ed.stanford.edu/news/stanford-researchers-find-students-have-trouble-judging-credibility-information-online

12   GSMA. "The Mobile Gender Gap Report 2020." 2020. Accessed July 2020: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/02/GSMA-The-Mobile-Gender-Gap-Report-2020.pdf

13   Pew Research Center. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information." 2019. Accessed July 2020: https://www.pewresearch.org/internet/2019/11/15/how-americans-think-about-privacy-and-the-vulnerability-of-their-personal-data/

14   For a rich discussion of the normative assumption of Western cultural values in technology design, see Sambasivan, N.; Checkley, G.; Batool, A.; Ahmed, N.; Nemer, D.; Gaytán-Lugo, L.S.; Matthews, T.; Consolvo, S. and Churchill, E. "'Privacy is not for me, it's for those rich women': Performative Privacy Practices on Mobile Phones by Women in South Asia." 2018. Accessed June 2020: https://www.usenix.org/conference/soups2018/presentation/sambasivan

15   UNESCO. "Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training." 2018. Accessed July 2020: https://en.unesco.org/fightfakenews

16   See, for example, Girl Effect & Vodafone Foundation. "Real girls, real lives, connected: A global study of girls' access and usage of mobile, told through 3000 voices." 2019. Accessed July 2020: (https://www.girlsandmobile.org/), or Sambasivan et al (https://www.usenix.org/conference/soups2018/presentation/sambasivan)

ACKNOWLEDGEMENTS

SHAPING A MORE LIVABLE WORLD.

___