“Your Protection is in Your Hands Only”: User Awareness and Adoption of Privacy and Security Practices in Five Majority World Countries

Rebecca Umbach, Anubha Singh, and Ashley Marie Walker

Abstract. Technology companies frequently develop and launch features to protect privacy, reduce user harm, and increase security. But adoption is inconsistent at best. Businesses might increase awareness through prominent placement on user interfaces or in-product promotions, and drive adoption through changes to default user settings, or by guiding users to tutorials that encourage them to engage with a new feature. These solutions can be effective but fail to capture key factors that inform use and adoption—particularly in the majority world. In this study, we conducted qualitative interviews with 24 participants in five majority world countries across three continents: the Philippines, Brazil, India, Egypt, and Nigeria (*N*=120). We assess the awareness and use of privacy and security features related to internet usage generally, and internet-connected mobile devices specifically. Participants often cited worries about being victimized by financial scammers, and highlighted how frequent sharing of devices, a common behavior, resulted in consistent concerns about privacy. We identify barriers and concerns around use and adoption for users in these regions and offer a holistic analytical framework that can be leveraged by actors in the space to better understand user behaviors and attitudes, and design accordingly.

1 Introduction

Trust & Safety is both a concept and a specific space within the technology ecosystem that refers to the people and functions that keep a platform safe, reducing user exposure to harms, fraud, and other online abuses. Trust & Safety teams often operate horizontally across company products to develop policies and enforcement processes to maintain a prosocial space and ensure companies adhere to the laws and regulations relevant to their users (Bhatlapenumarthy 2022). Areas that Trust & Safety teams may address, among others, include suicide and self-harm, mis- and disinformation, spam and fraud, non-consensual explicit imagery, and child sexual abuse material (Cryst et al. 2021). For example, Trust & Safety policy teams may develop guidance around permissible explicit content, enforcement teams may review user reports and feedback, and engineering teams may develop tools and models to moderate content at scale.

doi:10.54501/jots.v2i1.114

While there are critiques of ad-driven, data-collection revenue models that underpin many online spaces (Zuboff 2015), Trust & Safety teams have emerged as an important tool for maintaining a sustainable online environment for users by highlighting harmful dynamics and proposing potential solutions within the current operating paradigm (Bhatlapenumarthy 2022).

Maintaining online user safety falls to both platforms and users. Platforms have to wrestle with difficult content moderation decisions and make design choices to discourage bad behavior. Users can take proactive steps to protect themselves and their data. Depending on the platforms or products employed, users routinely, and often unknowingly, reveal a large variety of data about themselves, ranging from their interest in a sports team to their financial details. For instance, more than 190 million Americans use online banking services (Statista Research Department 2023). One consequence of this preponderance of available data is a corresponding rise in scamming and other types of online criminal behavior. Between 2019 and 2020, Google reported blocking over 100 million phishing emails daily through the use of sophisticated machine learning models (Kumaran and Lugani 2020; Kumaran 2019). In 2021, the Federal Trade Commission (FTC) received more than 2.8 million consumer scam reports, accounting for 5.8 billion dollars in reported losses in the United States alone (FTC 2022). Additionally, the Federal Bureau of Investigations received almost 850,000 complaints of cybercrime from the public in 2021 (ITRC 2022). Staying ahead of increasingly sophisticated scams requires technology companies to regularly develop improved and scalable methods to protect user data. Trust & Safety organizations are primarily charged with keeping a platform safe. However, the competency and functions of a Trust & Safety organization also influences users' perceptions of the ability to protect themselves and their data online. In addition to helping increase user trust in the platform, empowering users to protect themselves reduces harms, subsequent user reporting, and enforcement: an obvious operations cost-saving opportunity for technology companies.

Companies typically make features and settings available to all users regardless of geography, but uptake and adoption will vary widely based on a number of factors. Characteristics of the features themselves (e.g., whether it is forced through system requirements, whether it is opt-in or opt-out, and the level of complexity around the adoption process), external-facing behaviors of the tech companies (e.g., how it is marketed, what the release strategy is), and attributes of the users (e.g., age, internet usage, race, socioeconomic class, household structure, level of internet sophistication, level of concern about online victimization, etc.) may all influence user adoption (De Cristofaro et al. 2013; Zou et al. 2020). Unfortunately, many of the user attributes that are often related to lower uptake, such as age and socioeconomic or racial marginalization, are also risk factors for victimization (Pratama and Firmansyah 2021; Das et al. 2020; Ticona 2022). Compounding this problem, these vulnerable users also often experience higher consequences if victimized due to fewer resources or recourse options available (Ticona 2022).

For all of these reasons, online service providers, and especially the Trust & Safety organizations within those providers, have a vested interest in users being both aware of and willing to adopt the features built to keep them safe. One challenge is that many large technology companies are based in the minority world. (The term "minority world" is used herein for wealthier parts of the globe, which represent a smaller part of the world's population, including the United States, Europe, Australia, and Canada (Madrid Akpovo, Nganga, and Acharya 2018; Ponciano 2022); "majority world" refers to the world area in which most of the world's population live, including Africa, Asia, and Latin America (Powell et al. 2011)). These minority world-based companies may thus have biases or operational challenges resulting in (1) inequity in access for majority world users, both

to their platforms and to specific features within those platforms (Cheruiyot and Ferrer-Conill 2021) and (2) disproportionate exposure to harm for majority world users due to the difficulties in scaling a global Trust & Safety operation. Tangibly, this means majority world users may experience compounded harms (Gilbert 2020). For example, a report from Global Witness indicated that a pressure test of political ads on various social media platforms found lower levels of enforcement against policy-breaking ads in Brazil as compared to the United States (Normington 2022). An additional challenge is the reality that regulations around the world evolve at different speeds, and industry is accustomed to designing for and prioritizing users in countries with proactive regulatory environments. Nevertheless, those built products and affordances are deployed globally. The term "digital divide" was coined in the 1990s to refer to the gap in access to computers and the internet (Van Dijk 2006; Castells 2002). In the ensuing years, additional levels have been added: the second digital divide highlights the importance of digital skills and competency (James 2021), underscoring the inadequacy of simply providing access without the necessary support. The third digital divide refers to the returning benefits of using the internet, even with adequate access and skills (Aissaoui 2021; Ragnedda and Muschert 2017). As the first digital divide closes (Petrosyan 2021), technology companies are seeing millions of new users come online. They are now faced with addressing the second and third digital divide, helping these new users come online safely and use their services in a beneficial way.

In this qualitative study conducted by three researchers in Trust & Safety at Google, 120 one-hour interviews were conducted with participants across five majority world countries to better understand their privacy and security concerns. While the interview guide was semi-structured to allow the interviewers to pursue issues as they arose, all participants were asked about their knowledge and adoption of existing settings, features, and products that help protect users online (e.g., password managers, PINs, pattern lock). Participants were also asked about their concerns and how they thought about and retained their privacy online and on their devices.

Many of the behaviors and concerns voiced by users resembled those of minority world users, such as the desire to keep certain content private from others, worries about childrens' exposure to online harms, and a privileging of existing behaviors over the adoption of safer, but perhaps more cumbersome, new approaches. Despite these overlaps, specific behaviors, such as frequent mutual use of devices, highlight the fact that technology companies have to acknowledge they cannot build "one size fits all" features as solutions and expect them to be used equitably. Passwords are less useful when you expect to share an account and/or device, premium services that require payment may be out of reach for many users, and lower-priced devices may lack the capabilities for more advanced security features. Acknowledging the context of feature implementation allows companies to better plan for the culturally specific barriers and drivers of uptake that might limit the effectiveness of these new designs and, consequently, to develop appropriate interventions.

2 Background

2.1 Internet Technology in the Majority World

There is a robust body of work surrounding information technology issues such as privacy and security, particularly situated in minority world countries (Zou et al. 2020; Rainie et al. 2013; Milne, Rohm, and Bahl 2004; Baruh, Secinti, and Cemalcilar 2017; Boerman, Kruikemeier, and Zuiderveen Borgesius 2021; Trepte et al. 2015; Acquisti et al. 2017). There is also research conducted in the majority world; however, much of it focuses

on individual topics within technology, such as e-banking in Kenya (Gikandi and Bloor 2010) and the Philippines (Chiu, Chiu, and Mansumitrchai 2016), cyberactivism in Egypt (Ibrahim 2019; Tazi 2021), or the Internet Bill of Rights in Brazil (Rossini, Cruz, and Doneda 2015; Souza and Nunes 2022). This research aims to add to our foundational understanding of how users in the majority world conceptualize the risks of being online, and what strategies and practices they are aware of and use to protect themselves. This can help technology companies better anticipate trends in harms and design for more widely applicable protections.

2.2 Privacy and Security

There is a large body of literature spanning several disciplines discussing how people and users experience and conceive of privacy as a concept. For example, a distinction has been drawn between vertical privacy—that is, privacy from institutions, governments, companies, and so on—and horizontal privacy, which focuses more on privacy from individuals in ones' immediate circle and other people (Masur 2018). Additionally, there are several conceptualizations of why and how individuals make the choices they do with regard to their private or personal information. In the online space, especially, research has worked to explain why individuals engage (often knowingly) in risky behavior. The "privacy paradox" aims to address the inconsistencies between users' stated concerns and their actual online behavior (Kokolakis 2017). The "privacy calculus," primarily focused on behaviors on social network sites, extends the idea of a cost-benefit analysis to how users disclose information about themselves, or engage more widely, with social network sites (Dienlin and Metzger 2016). While much of this work has been conducted in minority world countries, consistent findings have been noted in work in Korea (Min and Kim 2015) and China (Cheung, Lee, and Chan 2015), suggesting at least some level of universality.

In considering specific choices or features available to users, research has often focused on the trade-offs between security and convenience, and the level of usability (Zou et al. 2020). Reluctance to use password managers has been traced to users' fear that they will be unable to access passwords when they need them, usability issues such as poor performance on mobile devices, or security concerns about the underlying product (Oesch et al. 2022; Pearman et al. 2019; Fagan et al. 2017). Research on biometrics has noted that even when both options are provided, participants prefer fingerprint unlock to facial scan unlocking (Bhagavatula et al. 2015; G. Cho et al. 2020) due to perceived benefits such as reliability. One study observed that because fingerprint unlock preceded facial scanning unlock, some amount of reluctance may be due to distrust of new features (Wolf, Kuber, and Aviv 2019). Research around web privacy tools has focused predominantly on the gap between user expectations and reality, specifically what misconceptions users had about the level of privacy provided by the tools (Gao et al. 2014; Wu et al. 2018). One notable related study (Frik et al. 2022) surveyed minority world users in underrepresented socioeconomic and low-tech groups to evaluate their awareness and configuration of various settings on their smart phones. They found that users often reported relying on strategies designed to help avoid risky behaviors rather than adopting more reliable protections; the authors note that this may come at an economic and/or opportunity cost to such users. Moreover, such strategies rely on the users' ability to accurately identify suspicious content. A significant minority of users also anticipated difficulties with changing the default settings, and many misunderstood what protections were offered by specific settings. In sum, many of these minority world-based studies demonstrate that despite some level of awareness about a vast spectrum of features and options, participants may eschew them for a variety of reasons including but not limited to misconceptions and convenience.

2.3 Sharing of Devices

There is a significant body of work on different aspects of device and account sharing, including user perceptions of sharing, and the factors that influence sharing behavior. Steenson and Donner (2017) distinguished between different types of sharing, namely distributed (e.g., where person A will call person B to reach person C, who lacks a phone) and proximate (where person A may share a phone with person B because they are together in the same location). Device sharing can be sporadic or frequent, and the level of comfort with sharing is likely to depend on a number of factors, including the type of relationship the sharer has with the "sharee" and the use cases of applications being exposed. Relevant to this study, which interviews participants in the majority world, much of this work has focused on the conditions that lead to device sharing, namely economic limitations and social values (Karlson, Brush, and Schechter 2009), and highlights the divide between how technology companies typically design features (e.g., one account/device, one adult user) and the lived experience of many users who may share devices with children, spouses, or other loved ones (Ahmed et al. 2019; Ahmed et al. 2017; Kelley, Cranor, and Sadeh 2013).

Indeed, previous research has noted that user awareness of privacy-protective features varies widely, and that privacy-seeking as a concept is itself deeply culturally dependent (Sambasivan et al. 2018; Ahmed et al. 2019). One difference between majority world and minority world participants may be the frequency of or expectations surrounding sharing. Indeed, in a study of 99 US households, none of the participants reported mutual use (as opposed to occasional borrowing) of phones (Matthews et al. 2016). Additionally, it seems plausible that majority world "sharees" might typically engage in what have been described as "high-comfort activities" (e.g., use of the phone to make calls, play games, etc.) if they are merely borrowing a phone, as opposed to low-comfort applications (e.g., voicemail, emails, files, text messages) (Karlson, Brush, and Schechter 2009). In minority world countries, sharing may be more sporadic or based on convenience rather than necessity (e.g., if the device owner directed a passenger in their car to reply to a specific text message while they are driving, if someone else's device has run out of battery) (Matthews et al. 2016). Retaining constant physical control of a device, retaining sole control over credentials, only granting sporadic use of the device under supervised circumstances, or intrinsic trust in any "sharee" may mean that app-level passwords or signing out of apps after use are perceived as unnecessary precautions.

In contrast, research across a number of majority world countries has shown more significant mutual use (Steenson and Donner 2017; Burrell 2010; Oduor et al. 2014; Donner 2006). In this case, the primary owner may limit independent access to the device as a tool of control, or alternatively grant a "sharee" much more access for the sake of collective convenience. We highlight the former scenario because these issues around control, particularly around the way that gender dynamics played an important role in access, were highlighted across a number of studies (Burrell 2010; Sambasivan et al. 2018). To some degree, tech companies have created features or protections designed to acknowledge sharing use cases. Certain operating systems or applications within operating systems acknowledge sharing use cases more than others, such as the guest mode available on Android, the availability of password-protected folders on Google Photos, or biometric-protected folders on iOS Photos. Most browsers now include a mode for browsing privately. App locks and password-protected applications also grant more control to the primary owner of a device, but may be of limited use depending on the sharing use case. Nevertheless, many of these solutions introduce friction at various steps that may cause the average user to skip the protections entirely. While technology companies may prefer that devices be single-user from a privacy and security standpoint, given the rate of even incidental sharing, it is critical to build settings or features to

accommodate sharing in an easy, low-friction, and privacy-protecting way.

3 The Present Study

In this exploratory study, we wanted to better understand how users in the majority world experience and think of Trust & Safety concepts online. This includes how users think of their own risk of victimization, what types of victimization are top of mind, how they learn of ways to protect themselves, and how they employ those strategies (or not). Many of these concepts are also related to common online privacy and security concerns. We recognize the prevalence of device-sharing, particularly in internet-maturing countries, so we probed on concerns specifically related to sharing. Relatedly, we note that we focus primarily on those settings and features that enable horizontal privacy, as opposed to vertical privacy, as those were top of mind for many of our users. We employed semi-structured interviews to answer the following questions:

1. What do users believe about safety online, and from where or how are they deriving that information?
2. What are the biggest concerns around online harms?
3. What are the barriers to adoption of features/settings and mitigation strategies?

4 Methods

4.1 Data Collection

We (researchers at Google) enlisted a dedicated research firm with global coverage to recruit and interview participants for the study. Semi-structured interviews were conducted entirely via video calls from December 2021 through February 2022. We took a phased approach, conducting the initial interviews in India with observation by one of the authors (fluent in English and Hindi) to ensure quality and to refine the interview guide. Subsequently, sessions were conducted by in-country interviewers in the Philippines, Brazil, Egypt and Nigeria. Participants were offered the option to take the interview in English or in the official language of the country, with simultaneous translation into English as needed so the authors could observe. Participants were given a nominal token of appreciation for their time. The research firm determined the amount based on local economic dynamics, but it ranged from $25 USD (India) to $50 USD (Egypt). We asked participants about their own safety habits and how they learn of different protective offerings. We asked respondents more specifically whether they knew about or used a variety of safety features and practices (listed in Table 1).

Table 1: Respondents were asked about their knowledge of and attitudes toward these features in interviews

Clearing Browser History	Clearing Cookies
Facial Lock	Fingerprint Lock
Guest Mode	Incognito Mode
Parental Controls	Passwords
Password Manager	Pattern Lock
Reusing Passwords	SafeSearch[a]
Using Strong Passwords	2-Step/2-Factor Authentication

a. A Google Search feature that allows users to filter out explicit content in their Search results

Most of the features listed here are available regardless of browser type and mobile device, with some exceptions (e.g., child mode, guest mode, pattern lock) that are only available on some operating systems or certain tiers of devices. Where appropriate, synonyms were provided (e.g., multi-factor authentication vs. 2-factor authentication vs. 2-step authentication). We selected several features that are universally available such as private browsing and alphanumeric passwords, as well as features that may address specific concerns or are limited to specific operating systems. For example, parents may be more knowledgeable about SafeSearch and parental controls, Android users may have more information about guest mode than their iOS counterparts, and users of mobile banking applications may be more knowledgeable about 2-factor authentication. This list is abridged compared to prior quantitative research (Zou et al. 2020) due to time constraints associated with interviewing newer internet users, many of whom needed clarification and additional descriptions of the assessed features.

4.2 Participants

Native language moderators conducted 120 (24 per country) hour-long, 1–1 virtual, semi-structured interviews in the Philippines, Brazil, India, Egypt, and Nigeria. We determined sample size based on ensuring sufficient coverage across our recruitment requirements, balanced with recruitment resources available in each country. We chose these countries for a number of reasons. These areas represent three continents in the interest of geographic representation, have high rates of scamming and victimization, and are relatively early in their internet maturity. Although participants were intentionally recruited from multiple majority world countries, our goal was not necessarily cross-country comparisons, but rather to identify the commonalities across a diverse group of users. Our screening criteria included a 50/50 split of men and women and an even distribution across three age quartiles. To ensure a wide range of participant sentiments, effort was expended to recruit newer internet users (less than three years of experience), as well as more experienced users. However, while we aimed to over-recruit newer internet users, just over 50% of participants had more than three years of internet experience. Our recruitment goals included regular device sharing by at least 25% of our participants in each country. All respondents had at least a high school education, but participant occupations remained broad, ranging from farmers to small business owners to students. A full breakdown of participant demographics are available in Table 2, and details of household composition are available in Table 3.

Table 2: Participant Characteristics

Variable	Group	% (# of Participants)
Age	18–25	25.0% (*n* = 30)
	26–35	25.0% (*n* = 30)
	36–45	25.0% (*n* = 30)
	46+	25.0% (*n* = 30)
Internet experience	<1 year	11.7% (*n* = 14)
	1–3 years	35.8% (*n* = 43)
	3+ years	52.5% (*n* = 63)
Gender	Female	50.0% (*n* = 60)
	Male	50.0% (*n* = 60)
Has 1+ child	Philippines	67.0% (*n* = 16)
	Brazil	70.1% (*n* = 17)
	India	54.2% (*n* = 13)
	Egypt	62.5% (*n* = 15)
	Nigeria	45.2% (*n* = 11)
Shares device w/ 1+ people	Philippines	25.0% (*n* = 6)
	Brazil	37.5% (*n* = 9)
	India	50.0% (*n* = 12)
	Egypt	70.8% (*n* = 17)
	Nigeria	25.0% (*n* = 6)

Table 3: Household Composition by Country

Country	Type of Household	% (# of Participants)[a]
Philippines	Single Occupancy	33.3% (*n* = 8)
	Married, cohabiting with no dependent children	0.0% (*n* = 0)
	Married, cohabiting with dependent children	54.2% (*n* = 13)
	Single parent family	0.0% (*n* = 0)
	Other multi-person household	12.5% (*n* = 3)
Brazil	Single Occupancy	20.8% (*n* = 5)
	Married, cohabiting with no dependent children	12.5% (*n* = 3)
	Married, cohabiting with dependent children	37.5% (*n* = 9)
	Single parent family	29.2% (*n* = 7)
	Other multi-person household	8.3% (*n* = 2)
India	Single Occupancy	20.8% (*n* = 5)
	Married, cohabiting with no dependent children	16.6% (*n* = 4)
	Married, cohabiting with dependent children	55.2% (*n* = 13)
	Single parent family	0.0% (*n* = 0)
	Other multi-person household	16.6% (*n* = 4)
Egypt	Single Occupancy	8.3% (*n* = 2)
	Married, cohabiting with no dependent children	4.2% (*n* = 1)
	Married, cohabiting with dependent children	66.6% (*n* = 16)
	Single parent family	0.0% (*n* = 0)
	Other multi-person household	20.8% (*n* = 5)
Nigeria	Single Occupancy	37.5% (*n* = 9)
	Married, cohabiting with no dependent children	12.5% (*n* = 3)
	Married, cohabiting with dependent children	41.7% (*n* = 10)
	Single parent family	0.0% (*n* = 0)
	Other multi-person household	8.3% (*n* = 2)

a. % sum may exceed 100 due to multigenerational households with dependent children

4.3 Research Ethics

Participants completed an informed consent form in their preferred language, and were asked to verbally consent at the beginning of the interview. Participants were made aware that they had the right to terminate the study at any point and could refuse to answer any question. Participants were informed that the interview was being recorded, but were offered the opportunity to turn off their video for privacy, to reduce the amount of data usage of the interview, or to improve connectivity issues. Participant quotes are anonymized using initials, gender, and age range. Participants were asked to take the interview in a quiet and private place. For the vast majority of users—and perhaps largely due to COVID-19—this meant they were interviewed at home.

5 Results

In this research we set out to better understand the safety and security beliefs and habits of internet users in majority world countries. We also develop a framework to better understand how the characteristics of privacy- and security-forward features and settings inform the likelihood of adoption. It is our hope that this framework can be used by technology companies and Trust & Safety organizations to inform product development and deployment. We set out to answer the following research questions and structure our results accordingly.

1. What do users believe about safety online and from where or how are they deriving that information?
2. What are the biggest concerns around online harms?
3. What are the barriers to adoption of features/settings and mitigation strategies?

5.1 User Beliefs about Risks and Safety Online and Whence They Derive

Much of the interview time was spent gauging how users felt about their privacy and safety given their particular circumstances (e.g., how they use the internet, how they currently protect themselves, who they perceive as potential bad actors). For most participants, threats or bad actors were those outside of their family and friend circle—strangers who could somehow obtain their devices or data. Participant threat models discounted the possibility of malicious acts by loved ones because there was high existing trust, and they gave little thought to how quickly circumstances or relationships might shift. Romantic partners were not thought of as threat vectors in any way, and there was low perceived need of privacy from them. Similarly, there was low concern about siblings and friends when it came to serious or malicious online abuse, but participants did express a desire to retain some privacy and many had mitigating strategies centered primarily around preventing access to messages and photos when sharing devices. The salience of device sharing, or physical access to their device(s), was also present when participants thought about bad actors. Bad actors gaining physical access to their devices was a concern, whereas remote access was quickly dismissed as unlikely, particularly if they had not clicked on links or actively disclosed their information. These salient concerns illustrate two things: (1) rather than trying to alter user perceptions of the threats posed by loved ones, perhaps the focus should be on creating resources and processes that are easily accessible and actionable should relationships dissolve; and (2) significant education is needed to inform users about the sophisticated ways that bad actors may remotely access their data and devices. Acknowledging individual and contextual variability (e.g., romantic relationships, living situations, previous victimization, geographical location, changes over time) regarding victimization and threat models illustrates there is unlikely to be a “one size fits all” solution for users. Instead, educating users about the risks and providing an assortment of accessible features and settings that can be tailored to unique situations may be the most realistic strategy for technology companies moving forward. While minority world participants would also likely benefit from tech companies accounting for these considerations, majority world participants in particular, who are more likely to share frequently, and with sharees who engage in “low-comfort” activities such as messaging, need features that reflect the lived reality of their device use.

5.1.1 Majority World Prevalent Sharing Behaviors

Many respondents were most concerned about the repercussions of someone else having physical access to their phone (as opposed to the possibility of remote access),

concerns perhaps exacerbated by the regularity of sharing behaviors. When sharing with siblings, friends, or even parents, concerns centered primarily around invasion of privacy, although not always explicitly stated as such. For example, K (Philippines, Female, 18–25) volunteered that while she shares her phone with her parents intermittently and they have the phone PIN, "*they don't know [the individual application passwords*." K specifically locked down her social media applications while allowing her parents to use her phone for messaging and gaming. Although privacy was top of mind, there was little concern for impersonation or financial fraud by those with whom they shared. Sharing with strangers was uncommon, but there were particular situations around content types that worried participants, such as M (Egypt, Male, 36–45), who was more concerned about the privacy of the women in his life than for himself: "*It is difficult to give your mobile to a stranger as they can open your gallery and they can see a photo of my sister or my mother without a veil*."

Many participants took steps to mitigate the risks associated with device sharing. Participants often either had defined rules or strategies for the people with whom they shared their device, or adopted technical safeguards to limit access to content on their device. K (India, Male, 18–25) said he did not bother to lock his Facebook and Instagram accounts, which he was fine with his younger siblings accessing, but password-protected his WhatsApp app because "*I don't want to show my WhatsApp to them*." Alternatively, R (Egypt, Male, 46+) actually physically managed how his friends handled his phone: "*I never allow [friends] to open an application, I hold my phone when I give it to them*." M (Egypt, Male, 36–45), who was concerned about his friends checking his photos, used technical solutions like app locks to limit friends' access to their photo applications. Although participants ranged in their frequency and level of sharing, most had adopted personal strategies to mitigate the perceived risks.

One exception to worries around sharing was the lack of concern when sharing with romantic partners. This was exemplified by L (Brazil, Female, 18–25), who had registered her husband's fingerprint on her own device despite not using that feature herself: "*On my phone [my husband] has a fingerprint, so he uses it. I don't really like fingerprints, it's a lot of work*." E (Brazil, Male, 26–35) explicitly rejected facial recognition in favor of a PIN code known to his wife because "*[if I use facial recognition] it will complicate things and create a distrust...between me and my wife*." Notably, there was little to no mention of explicit monitoring by other adults, a practice previously documented in other studies focusing on female experiences in majority world countries (Sambasivan et al. 2018; Sambasivan et al. 2019). While sharing can occur in a prosocial and safe way, the ubiquity of incidental sharing underlines one pathway for harm that is worthy of additional user education (Dragiewicz et al. 2019; Woodlock 2017; Henry, Flynn, and Powell 2020; Ibtasam et al. 2019).

5.1.2 User Beliefs

Users also held strong beliefs that if their devices and applications were password protected, and if they took basic precautionary measures like ignoring unsolicited links, they were safe online from bad actors. That is, while they were concerned about and aware of the risks of disclosing their information to scammers through phishing strategies, they typically discounted the possibility of brute-force hacking. This mental model is exemplified by G (Egypt, Female, 36–45), who said, "*Everyone is worried about hacking, but for me I do not press on any links*," and A (Philippines, Female, 46+), who said, "*I see some posts of my friends saying 'Hey don't message me on Facebook because I'm not the one who's using it because my ID was hacked' the thing that comes to my mind is how can they hack it if you don't give your account?*" A went on to say, "*I am reassured because I have passwords, the fear is that someone will take the cell phone, steal it and*

take something personally. Regarding [remote access to] my phone, I feel safe because of the passwords I put on it. It's only in case of theft that I don't feel safe."

Unfortunately, while this does mean many participants were aware of phishing and common scams, it did not occur to them that reusing passwords may leave them more vulnerable to remote abuse in the event that even one account gets exposed. This belief that a user must actively do something to leave themselves vulnerable to remote access (e.g., disclose login details, click links) may also lead to shame on the part of those who do get scammed. This demonstrates a need for nuanced, nonjudgmental education about the variety of ways in which scams are perpetrated and the risk factors that can lead to victimization online. Such an approach can help reduce victimization, as well as promote compassion and lessen shame for those who are scammed. Research in other fields (e.g., Spencer et al. (2017) and Lichtenstein and Johnson (2009)) suggests destigmatization should promote more willingness to disclose and self-report victimization, improving our knowledge and data of the prevalence of harm.

5.1.3 Sources of Information

To better understand the learning models of participants and the origins of their beliefs, we asked where and how they would learn of new technology issues, whether it be scams, features, or best practices. We then asked which sources they found most trustworthy. Mainstream media, social media, and word of mouth were the three most-cited sources of information, although there were differing levels of trust for each, with more mistrust of information found on social media compared to mainstream media and word of mouth. This view was expressed by A (India, Male, 46+): "*[I'm not always] trusting the things on social media because at times wrong things also would be shared there*." Word of mouth included friends and family, as well as employees in tech-related fields (whether employees at cybercafes, or even in-house IT colleagues of participants who worked office jobs). V (Brazil, Male, 46+) explained: "*The IT people are willing to take information and disseminate it in the company, this for us is very good because most are computer illiterate*." M (Brazil, Male, 25–34) had confidence in the mainstream media to tell him when there was new information he needed to know: "*When it is [important] information it appears there in the news and through television as well, through the G1 [local news] channels*." S (India, Male, 18–25) echoed this sentiment: "*Through TV and newspaper only, that is the maximum [important source]*."

Across countries, participants often described a learning journey wherein they would hear of a phenomenon or problem via social media or through word of mouth, and would then trust the story only when validated by mainstream media.

5.2 Biggest Concerns around Online Harms

We asked participants what they worried about most when it came to their device and when using the internet. We did not ask participants to rank a set of concerns, and as such, the concerns outlined in this section are not in priority order. Universally, participants were concerned about potential financial harms deriving from bad actors gaining access to their banking information. Participants also worried about scammers impersonating them (either through the creation of a duplicate account or through hacking into their true account) and either posting bad content to damage their reputation or using that access to scam their close friends and family. The participants who had children in the home highlighted concerns about potential harms that the child(ren) could experience, particularly around exposure to inappropriate content. Finally, and unsurprisingly given the rate of frequent sharing reported, participants were apprehensive of the potential for

sharees to access private content, including photos and messages (notably "low-comfort" activities (Karlson, Brush, and Schechter 2009)).

As noted, there are strategies these participants can take to mitigate these risks themselves, but it is worth noting the additional parties that may be involved, or that the existing options are inaccessible or so inconvenient as to render normal activities overly burdensome. Concerns around financial scamming involve financial institutions that may force their own requirements (e.g., multi-factor authentication, strong passwords). The impersonation problem mostly falls under the remit of the social media companies and was considered a growing problem even in the earliest days of social media (Reznik 2012). The parental concerns are reflected in the increasing regulatory scrutiny regarding age-appropriate content and protections (ICO 2020). Most of the participants listed one or more of the aforementioned worries when probed on their greatest fears and concerns about their internet use.

5.2.1 Phishing and Financial Scamming

Many participants mentioned foiling a scamming attempt, but few reported being personally victimized. There seemed to be relatively widespread awareness of the most common types of scams, such as phishing or impersonation of officials or loved ones, and this type of information is shared by trusted news sources as well as by word of mouth. For example, M (India, Female, 36–45) said that she had heard "*in the news and in my friend circle and neighboring people [who] keep telling me that when you have phone calls at that time you should not share your information. My kids also tell me that don't attend any unknown number and don't share your OTP [one time password] with anyone*." M got to put this advice into practice when a scammer contacted her with a lottery scam:

> *I got a call stating that you have won 20 lakhs rupees and if you give your account number we will transfer money to your account and plus give 4k rupees and so I told them to deduct 4k and give me the remaining amount. I told him if you want to deduct more than that also so you can deduct that also and they said them give your account number. I told them give me cash, come [to my] home and give me the lottery amount in cash, I don't share my account number with anyone.*

C (Philippines, Female, 26–34) claimed that she knew better than to fall for scams, except for the one time she fell prey to a scammer impersonating her mother, who asked her to load (i.e., top-up) her pay-as-you-go phone: "*Sometimes your 'mother' will tell you 'I had an accident can you send me load?' I never entertain that but one time it happened to me…I [didn't realize] that it's a fraud so I got to pass a 500-peso load to that person*."

Users seemed to perceive these types of attempts as the cost of being online, with those who were scammed resigning themselves to the loss. The juxtaposition of C claiming that she never falls prey to scammers, immediately followed by her chagrin in recounting a case in which she did, speaks to a potential side effect of the ubiquity of certain online financial scams: users seem both confident in their ability to identify them, and ashamed to admit when they are victimized.

5.2.2 Impersonation

Many participants had either fallen victim to or seen friends fall victim to hijacked accounts on social media. One area of concern was how scammers could use their

account to damage their reputation, either by financially scamming others in their circle, or by posting abusive content, as M (Philippines, Female, 36–45) said:

> *My information could be used in other countries as a form of identity. They could be used for scamming, with your pictures, your name. For example in dating apps they could use their photo. Or on Facebook or Instagram, when posting, that identity can be used by other people to scam others.*

A bad actor could gain access to social media accounts either remotely or through physical access, and there was little explanation from users about how they thought the bad actor would gain access. Once accessed, however, the time required to enact harms via others' accounts is negligible given the instantaneous nature of messaging and posting.

Scammers duping others and posting bad content are both concerns about reputational harms, which could happen to anyone regardless of the amount of information shared on social media accounts. Given that a main internet use case of the majority of respondents was social media, unsurprisingly some noted the potential that hackers would leverage private details from social media accounts, and leak that information or use it to blackmail the affected user. M (India, Female, 36–45) explained: "*Blackmailing is also going on and on social media there are people who say wrong things and they do so many wrong things by leaking their photos and at every place sharing all the information*." Participants also conflated actual hacking with duplicate accounts, where scammers never actually gained access to an account, but instead created impersonation accounts. D (Philippines, Female, 26–35) said, "*I think it's like hackers now, they would create scandalous things, for example…they would ask for money, even though it's not them. I think it's really bad because they can ruin the image of the person [they impersonated] even though they are innocent*." A (India, Male, 46+) echoed this:

> *With one of my friends, his Facebook account was hacked in 1 or 1 and half months back. So, he called me and told me that by using his name someone has created a duplicate Facebook account, please don't follow that account…If that hacked person will send some bad messages or photos to his friends or relatives, then his friends and relatives will think that it was sent by him only, so he messaged all about his duplicate account*.

Once victimized, some mentioned ways to remediate through the official channels of the affected account, although others were unaware that this was an option, like A (Nigeria, Male, 46+) when his Facebook was hacked and the hacker was messaging his connections demanding money: "*I couldn't do anything [after the hacking], who should I report to? Is there anybody I can report to that they hacked my account?*" While social media platforms have ways to report duplicate or impersonation accounts, the user is at the mercy of their turn-around-time and decision. Perhaps unsurprisingly, then, when asked to detail what steps they would take in the event of victimization, participants focused primarily on how they would rapidly notify their network of the breach rather than on what they could do via official channels.

While some participants cited examples of remote bad actors creating or hacking accounts, D (Philippines, Female, 26–35) was more focused on the likelihood that unauthorized access may occur based on the physical loss of her phone, which introduces additional complications to the notification and recovery process when a user does not have a secondary way of accessing the internet such as a laptop:

> *[I am most concerned about Facebook] because that's where they can easily access information and it's connected to Messenger so they can have access*

> *to my friends and they can do a scam. I think [if it happened] the best thing is if I can just log in, for example, even if—maybe just to rent a computer—to deactivate the account right away, I think that's possible and then just post right that I lost my cellphone so whoever sends you a message using my account regarding what matter just ignore, do not pay attention because I lost my phone.*

While many information and communication technology (ICT) companies have account locking or recovery mechanisms, triggering them typically requires internet access. Losing your phone may not present a problem for wealthier users, but could be a significant blocker for lower socioeconomic-status users whose only internet access is through the lost phone.

It is predictable that internet platforms provide a perfect storm for reputational concerns and scamming—social media platforms in particular encourage users to publish personal information on their platforms and have messaging capabilities (increasingly encrypted) to allow for conversations. This, in addition to user experience design that encourages identifying close friends or family, means bad actors can both easily map likely prospects and contact them surreptitiously. Many platforms have acknowledged this risk and introduced friction methods through design, such as separate inboxes, to avoid letting people outside of one's social circle to reach out seamlessly via direct messaging. Innovations such as verification are increasingly offered (e.g., X Premium [formerly Twitter Blue], Meta verification) (Korn 2023; Twitter Help 2023) but require payment on the part of the user, which may leave low-income users increasingly vulnerable.

In short, social media platforms often grant bad actors the information (e.g., close friends and family to target, personal data) and the tools (instant and direct messaging/posting/voice calls) to leverage victims' reputations for scamming and harm. Nevertheless, users seemed to feel significant personal responsibility both in safeguarding against the initial bad actor access, and in mitigating harms should they fall prey to such an event.

5.2.3 Children: Inappropriate Content Exposure and Incidental Data Exposure

Participants with minor children (either their own, or younger relatives) in their household often allowed the children to use their device for entertainment purposes or for their educational needs. Kids were usually told to stay on "safe" apps and games, and what content was inappropriate for them. Participants' stated concerns fell into one of three categories—and often more than one: **exposure to inappropriate content**, as expressed by D (Philippines, Female, 26–35): "*[Internet use can be] really dangerous for kids because they could see a lot of inappropriate things online that are not suited for their age, because in Facebook there are a lot of explicit posts that shouldn't be seen by kids*"; **accidental accessing of messages or exposure of private information**, such as the instance described by A (Egypt, Male, 25–34): "*[my nephew] once posted a story on WhatsApp that was confidential and I would not have post[ed]*"; and **fear of predators online**, as described by O (Nigeria, Male, 46+): "*My biggest concern [for my daughter] is communication with strangers; I try as much as possible not to leave anything that will allow communication with strangers*." There was little concern expressed about other topics surrounding childrens' internet use such as cyberbullying or developing healthy digital habits.

Despite numerous concerns for the online safety of the children in their lives, most of the participants were unaware of parental control options that could help them safeguard

children against these issues. Most had come up with their own mitigation strategies, ranging most commonly from physical supervision while their kids used their devices, as described by O (Egypt, Male, 18–25), "*I watch with [my brother] because there are ads that are not appropriate for children*," to disabling internet connectivity to eliminate the possibility of their children accidentally seeing incoming messages. S (India, Female, 36-45) said, "*I tell [my daughter] not to play anything when the net is on, I tell her if you want to play then switch off the net and then play what you want to play. It is because if the net is on then there can be some fear about what message[s] can come*."

Some participants did mention technical measures targeted toward parental pain points. Family Link, a Google feature that allows parents to manage their children's accounts, is one such option. While Family Link can block applications in their entirety, if you want your child to have access to apps but not to all the content within those apps, manual supervision is necessary. This inconvenience was encapsulated by C (Philippines, Female, 26–35), who explained that after registering for Family Link, "*the problem is each time 'mama I need to open the internet,' and I'm busy, so I approve it. Instead of not allowing him I ask my sister to supervise him on that*." Beyond account management, applications or platforms may have varying levels of age-specific programming and built-in restrictive features. Parents are likely to have their own philosophies as to what their child should consume and at what age, and these "one size fits all" approaches are unlikely to be satisfactory. Despite the many existing parental control features that services have developed and continue to invest in, most participants were unaware of these features. The interviews suggest participants were more likely to adopt their own mitigation strategies to keep the children in their lives safe from online harms.

5.3 Barriers to Adoption

Once aware of an available feature or setting, users then choose whether or not to use it. The study participants rarely changed their existing practices, particularly if they thought of them as effective (e.g., nothing egregious had happened that was directly attributable to something they were doing) and convenient. This is consistent with the general belief that falling victim to a scam requires active "participation" by the victim. By this logic, continuing with the status quo felt safe to participants, who were also reluctant to adopt new practices if the new practice was not perceived of as reliable, trustworthy, or more convenient. We have synthesized responses into the following themes as barriers to adoption:

- Perceptions of inconvenience
- Dependency on learning support
- Distrust of the novel

We also note that many of these could be extended beyond safety features online, to general practices in the physical world (e.g., those who don't lock their front door because they think they live in a safe neighborhood and worry about locking themselves out).

5.3.1 Perceptions of Inconvenience

Participants were willing to trade lesser security (especially if they had not personally had a bad experience) for greater convenience. JC (Philippines, Male, 26–35) exemplified this attitude: "*At the end of the day, you want more convenience over safety in using your gadget…You only realize the importance of security or safety when you're hacked, or your phone is lost or stolen*." For example, many reused the same password across different

platforms and on different accounts to avoid having to remember unique passwords each time they have to log in (Wang et al. 2018). As A (Philippines, Female, 36–45) put it, "*when passwords are different for each app, it is much safer but for me, for my memory, I only use one*," a sentiment echoed by J (Brazil, Male, 36–45): "*I don't switch [passwords…there are so many passwords, cell phone passwords, bank passwords, Facebook passwords, email passwords, if you change them, you have to keep changing and writing down the new passwords because it is a lot of information*." Those who can't re-use their typical password due to system or platform requirements may use different permutations of the same password.

Even participants who understood that reusing passwords left them vulnerable were unwilling to adopt ready solutions, such as a digital password manager. In general, when asked how they kept track of passwords, participants across regions often cited documenting them in a separate location, either analog or aggregated in online note form, as A (Philippines, Male, 18–25) did: *"[I don't forget my password], because when I create an account, I usually copy it in a notebook*." Similar to the parental strategies discussed in Section 5.2.3, many of the participants defaulted to habitual strategies rather than taking advantage of purpose-built options. While many tools have been designed to eliminate problems such as password management, the uptake of such tools has been relatively low (Alkaldi and Renaud 2016), indicating the need for more research into successful implementation strategies to improve uptake and overall password hygiene.

5.3.2 Dependency on Learning Support

Even when participants had heard of a new feature or setting, some reported needing assistance to understand them. Common problems included downloading a new application, updating existing settings, or understanding app permissions. Participants, especially older ones, were often reliant on others such as younger relatives or "experts" (e.g., cybercafe employees, the IT department at their jobs). D (India, Female, 26–35) explained: "*One of my brothers is a software engineer and his wife is also a software engineer, one makes the software and the other will test the software. So I will ask them…what all I can do. I will ask for their help*." When participants want to actively seek out information or find a solution for a problem, they often turn to trusted sources in person, like S (Egypt, Male, 18–25): "*I go to my nephews, one of them is a telecom engineer, so I ask him about dangerous things like that. I explain the situation to him and ask him what I should do, so I ask the expert*." A (India, Male, 46+) also consults perceived experts: "*I came to know about [transferring files to a USB flash drive] from a cybercafe. When I want to get some information regarding mobile, I use to go there and ask them about that. From there I [learned], that we can transfer our photos, videos to a pen drive, it is safer than having it on mobile*." This need to consult with perceived experts reflected participants' own beliefs around their lack of tech competency.

Ironically, depending on the context, parents and relatives quickly switch between feeling a need to supervise technology use by children, to depending on them for assistance and tech support. This sentiment was expressed by E (Brazil, Male, 26–35) when referring to his 10-year-old son: "*Because I don't understand much about the internet sometimes I ask my son [for tips] because kids nowadays know more than us*." A (Philippines, Female, 46+) gave a discrete example of a time when she asked her son for assistance in adopting a new feature: "*My son just taught me [how to use fingerprint unlock] . I said, 'Son, what's this, can you teach me how to use fingerprint locks?' then he taught me how to do it*." The idea that the younger generation is more informed and knowledgeable about the internet, together with the reality that much of their social and educational experience is now spent online, makes it even more difficult for parents to feel comfortable with their children's technology use. Shifting roles may make it harder for parents in a range

of areas, including maintaining authority over device or platform use, or acting as a knowledgeable source in the event that their child does experience online harms.

5.3.3 Distrust of the Novel

Many participants were suspicious about the reliability or value of new features. The low adoption of biometrics, despite high awareness, is a good example of how these features were sometimes perceived to be more cumbersome than helpful, with the added disadvantage of perceived security vulnerabilities. Compared to some of the beliefs listed above, these concerns were relatively well-founded (Bhagavatula et al. 2015). Participants noted that if your hands were wet or dirty, then the fingerprint matching would error out, presenting an unnecessary nuisance. O, (Nigeria, Male, 46+) explained:

> *[Sometimes if] you have something on your finger, it might not come up quickly, there are times when you have to try and try and it will tell you too many attempts, so if you are in a hurry, it will limit you…maybe the surface is dirty, maybe it's my fingerprint that is dirty, it will say wrong, adjust and when I try it will just say too many attempts, at the end of the day I will have to go back to password, so when I first open it and it brings fingerprints, I'll just cancel and go directly to password.*

Several were concerned that if you were sleeping deeply then fingerprint unlock could be used without your knowledge. J (Brazil, Male, 36–45) said "*The fingerprint you just have to put it and you have access, and the owner is sleeping*." This sentiment was repeated by F (Nigeria, Female, 26–35): "*Anyone can take your phone when you are not around or that you are sleeping…I started hearing that someone can use your fingerprint to open your phone when you are sleeping but if you have a password, nobody is going to open your phone even when you are sleeping*."

Participants expressed concerns about the level of accuracy in both directions when asked about facial recognition unlock. Participants thought it could be used by bad actors to access a device or app; they also worried that it could be buggy and lock out the user, despite the fact that alphanumeric PINs are required as backups when biometrics are in place. M (Philippines, Female, 46+) expressed a concern that a slightly changing appearance day to day may break the feature: "*you have makeup or glasses—it would hardly recognize you*." Access may also be impaired by the technology's ability to navigate environmental conditions, as E (Brazil, Male, 36–45) put it: "*If you're in a dark place, for example, you won't be able to unlock a device or an app by face. And with the password, you can do it, even if you are in a place that doesn't have much light*." Participants were concerned that facial recognition could be used without the participants' knowledge, or were concerned about the possibility that the device would be rendered unusable or inaccessible if the primary user became unavailable. Concern around permanent inability to access was vocalized by O (Nigeria, Male, 46+): "*[If I use facial unlocking] there is no way [my wife] can improvise [if a] bad thing were to happen, like a serious accident or death. In that case, nobody will be able to access the phone, so I would rather prefer something simple*." F (Nigeria, Female, 25-34) said, "*…it's not protective enough because even when you are sleeping, your phone can still recognize your face… That's just the disadvantage it has*." Many of these participants expressed beliefs or cited experiences that may be time and/or operating system specific. As ICT companies release features, it is often the case that they may have bugs or issues that are resolved in future updates. One downside of such an iterative approach may be that users have an initial buggy experience, and continue to index on that experience even after the issues have been resolved.

Notably, no users expressed worry about the possibility of governments or companies misusing biometric data. This issue has been debated by privacy advocates and scholars since before the advent of smartphones (Jain and Kumar 2012; Woodward 1997) and was salient during the summer 2020 Black Lives Matter protests (Chaudhry and Krasnoff 2022). Increasing awareness is not a requirement of tech companies, but if certain settings or features have the possibility to endanger users or enable unwanted access, those risks should be readily communicated.

In this section, we have summarized the barriers to adoption identified by participants. In exploring the importance of these barriers, however, there are two main considerations: ease and costs. Some of these barriers are easier to overcome than others. Distrust of the novel, for example, could be addressed through public awareness campaigns, and challenges around onboarding and educational materials are essentially a resourcing effort. Others are more challenging and speak to cognitive biases that exist across literatures and domains, such as normalcy and optimism bias. As far as importance, the Swiss cheese model (Reason 1990) seems applicable here. As long as users are using PINs and strong, varied, passwords, biometric unlocking is merely a convenience. If applications enforce OTPs or multi-factor authentication and users know not to share those, attempted hackers will be unsuccessful even when armed with login credentials. Acknowledging and anticipating user attitudes can help companies develop products for high adoption and market them appropriately.

5.4 Framework of Feature and Setting Adoption Characteristics

Thus far, we've focused broadly on users' beliefs and concerns, and highlighted a set of relevant features and settings that can help support the privacy and security needs of users online. Delving deeper, we distilled participant responses into three categories: high awareness and high usage, high awareness and low usage, and low awareness and low usage. This framework can help guide technology companies and other key stakeholders both in the development of new offerings and in the marketing or education strategies for existing ones.

Table 4: Framework for Adoption

Well-Known & Well-Used	Well-Known & Less-Used	Less-Known & Less-Used
Long-standing (e.g., alphanumeric passwords)	Useful at multiple levels (e.g., biometric unlocking)	OS/product specific (e.g., parental mode, guest mode)
OS/product agnostic (e.g., clearing your browser history)	Significant reliability improvement over time (e.g., biometric unlocking)	Requires user opt-in (e.g., private browsing)
System requirements across multiple popular/high-use platforms (e.g., 2FA)	High user burden with low perceived improvement (e.g., changing passwords frequently)	Unlikely to significantly change experience (e.g., SafeSearch)
		Additional cost (e.g., third-party password managers)

Developing this framework around the characteristics of digital features and settings helps illustrate two key points. First, simply building tools for users will not result in

widespread adoption, and may in fact result in inequitable adoption without additional intervention, compounding exposure of the most vulnerable users. Second, technology companies have demonstrated an ability to cooperate with rivals for specific issues (e.g., child safety via The Tech Coalition). Of the characteristics of highly adopted options, an obvious lever is designing them to be platform-agnostic and cross-platform. Replicating and expanding the aforementioned current cooperative efforts may help in securing online spaces for a wider range of users.

6 Discussion

We interviewed 120 participants in five different countries to learn more about their awareness and adoption of various features designed to increase their security and privacy online. This exploratory research was conducted during the COVID-19 pandemic, when participants were more likely than ever before to be restricted in their movements and dependent on technology to manage their everyday activities. There is a rich body of existing literature on concepts central to this study, including the privacy paradox (Kokolakis 2017; Gerber, Gerber, and Volkamer 2018) and attitudes around sharing devices and/or accounts (Steenson and Donner 2017; Karlson, Brush, and Schechter 2009; Sambasivan et al. 2018). This study demonstrated that across five countries representing three continents in the majority world, users surfaced many of the same concerns and employed many of the same strategies.

We aimed to approach these topics from a broad Trust & Safety perspective, with a goal of developing insights for tech companies to inform the development and lifecycle of protective features in an inclusive and accessible way. We note that almost all of the participants had either personally experienced, or more commonly, had someone close to them experience, a significant online harm—ranging from financial scamming to reputational harms due to impersonation. Despite awareness of and concern about potential harms, participants largely avoided newer options in favor of the practices they were familiar and comfortable with. This is in line with the privacy paradox (Barth and De Jong 2017; Kokolakis 2017; Gerber, Gerber, and Volkamer 2018), and indeed favors the privacy calculus (Dienlin and Metzger 2016), in that even those who have been harmed make choices to retain practices to which they are accustomed, and which remain convenient. This reluctance to adopt new practices is consistent with the literature surrounding minority world participants (Kokolakis 2017; Gerber, Gerber, and Volkamer 2018); however, the general awareness of options appears lower in these majority world participants.

Tech companies have increasingly acknowledged that protecting users with more advanced technology will likely also require a focus on convenience (Apple 2023), a strategy well exemplified by the recent collaboration between Microsoft, Apple, Google, and other tech companies to move toward a universal FIDO system that would reduce the reliance on passwords and work cross-platform (Ulqinaku et al. 2021). Nevertheless, users are typically nudged to adopt certain practices, rather than forced. Exceptions can be found in the financial services space or more generally across verticals when it comes to remote abuses (e.g., password strength requirements) . Additionally, in areas where companies have strong confidence in user preference, companies may make protections opt-in by default (e.g., blocking of phishing emails by Google, (Kumaran 2019)), straddling the space between simply offering a feature or setting and forcing users into it. Further, regulatory bodies may require better practices. For example, the Reserve Bank of India now requires multi-factor authentication for internet and phone banking to mitigate financial abuse (Reserve Bank of India 2021), a risk and solution highlighted by American governmental agencies in 2005 (Federal Financial Institutions Examination Council

2005).

Individuals who shared devices with partners were unconcerned about sharing, and typically took a stance that they had nothing to hide from those partners. This often went beyond simply allowing unsupervised use to explicit sharing of passwords or biometric access. Those who shared with siblings or friends were often more circumspect, expressing some concern about privacy and mitigating the risk through the use of app locks or physical supervision. Participants were primarily worried about others accessing messaging and photo apps. Few participants were aware of guest mode or other system-wide features designed to protect privacy in the event of multiple users sharing a single device. Although sharing is not intrinsically harmful or risky, circumstances may quickly make it so. Educating users about the risks, as well as ensuring they have insight into how to share in as privacy-preserving a way as possible, can help prepare users in the event of a crisis.

Many of the participants in our study shared their device regularly with their children, for both entertainment and educational purposes. Like parents in the minority world, participants with children in the home expressed concerns about children experiencing incidental exposure to mature or violent content (Danet 2020), and about the possibility of the children disclosing information about themselves or their family members inappropriately (Kumar et al. 2017). While the extent of screen time has long been a concern of medical organizations (Hill et al. 2016) as well as parents (Wiederhold 2020), there was relatively little stated concern by participants about extensive screen time, an issue potentially mitigated in this participant pool by lesser Wi-Fi access, different societal attitudes toward screen time, or lower rates of children having their own personal devices. Parents had various strategies to ensure their kids were staying safe online, but most relied on physical supervision and were relatively unaware of dedicated settings of features.

We highlight too, the impact of the second digital divide. While some of these participants, particularly the younger ones, did go online and do research themselves, many of the other participants relied on trusted sources who could provide 1–1, often physical, assistance in learning about and applying new features or options. Scholars have already noted that marginal internet users are often subjected to technology with little to no say over how their data is used (Gangadharan 2017). One step toward closing the second digital divide involves developing easily understood and reliable features and settings, paired with dedicated and accessible educational and marketing materials.

It is important to acknowledge that certain practices or features designed to protect against common issues may have their own issues, requiring even highly sophisticated users to weigh the costs and benefits of adopting a specific practice. These calculations may include the risks associated with entrusting sensitive information to an additional third party, e.g., a dedicated password manager company, or it may simply be time consuming, such as the user who attempted to password protect the browser app for her child just to realize it was highly inconvenient for her to approve each separate occasion. These concerns are also borne out not only by existing research, but by real-world events. Several high profile breaches of password manager companies in 2022 reinforce research demonstrating the risks of using password managers (Pearman et al. 2019) and have illustrated the reality that, depending on the household circumstances, the analog practices of many of the participants in this study may be safer than the more technologically advanced alternatives (Lyles 2022). Private browsing modes are now available in the majority of web browsers, but saw little uptake in this study; however, research has shown that the actual protections provided by such modes fall short of user expectations (Wu et al. 2018; Gao et al. 2014). Participants did not mention potential privacy concerns associated with the use of biometrics, a topic

long-discussed in ICT literature (Woodward 1997), but concerns about the legitimacy of judicial or law enforcement systems may give users understandable pause before enabling these technologies (Smith 2019; Kostka, Steinacker, and Meckel 2022). This reality complicates assigning a "positive" or "negative" valence to all of the choices made by participants in this study. Nevertheless, informed decision-making by users should improve equitability and reduce overall online harms.

Although this study was not designed to be COVID-19 specific, we would be remiss not to acknowledge the ways in which COVID-19 may have changed online behaviors and influenced responses to our research questions. The COVID-19 pandemic resulted in significant changes to how much of the world operated and saw a rise and evolution in both internet use (Feldmann et al. 2020) and online harms (Nolte et al. 2021; Wood, Hengerer, and Hanoch 2022; Stock 2020). Most countries enacted lockdowns of varying severity and length. One study estimated that over a third of the global population existed under some degree of movement restrictions by early April 2020 (Koh 2020), and another estimated that 1.75 billion students were affected by full or partial lockdowns (Oloyede, Faruk, and Raji 2022). Most had to rely on technology to safely stay connected, complete work, attend schooling, and communicate with loved ones. Additionally, as people spent far more hours in their homes than they had previously (Hanibuchi, Yabe, and Nakaya 2021; Bullinger, Carr, and Packham 2021; Aruga, Islam, and Jannat 2021), they necessarily conducted more of their lives online, often in conditions of decreased privacy (Baird et al. 2020). Unsurprisingly, given all of the above, cybercrime related to COVID-19 proliferated, including scamming through online impersonation, (Kikerpill and Siibak 2021; Abroshan et al. 2021; Lallie et al. 2021), targeting of support platforms and critical infrastructure, and fraudulent offerings of cures (Lallie et al. 2021). Technology companies had to rapidly tailor policies and enforcement to meet this surge in abuse; Google blocked nearly 18 million phishing emails per day related to COVID-19 in mid-April 2020 (Tidy 2020). COVID-19 acted as an exogenous shock, facilitating the conditions for a target-rich environment and allowing scammers to leverage fear of an unknown disease. We acknowledge the unique circumstances during which this study was conducted, and that it intentionally included participants with characteristics that may make them more susceptible to online abuse at a time when such abuses were on the rise.

6.1 Limitations and Future Research Directions

This study had several limitations. Given the public health risks of asking participants to leave their home during a pandemic, participants generally took the calls from a quiet and private space in their home; we asked participants to make sure the scheduled time was one in which they would feel safe in responding. Still, it is possible that concerns around monitoring or being overheard could have resulted in underreporting, both of concerns and of making use of features (e.g., private browsing).

Although it was not a prerequisite of this study that participants use a smartphone, all of the participants did, even those who had only been using the internet for less than a year. The majority of our participants only accessed the internet using mobile phones; laptop ownership was rare. From a resourcing standpoint and because of the scale of this research, more intensive recruitment of non-device owners was not possible, but future research could recruit feature-phone users to see how users conceive of privacy and security when their phones are not immediate gateways to as much personal information. Similarly, we did not intentionally recruit for people who had previously experienced specific harms or scams. Future research should explore how people in majority world contexts and low resource environments have responded in these kinds of situations.

In any self-reporting, there is the potential delta between reported behavior and actual behavior. It is possible that participants were in fact using certain features (e.g., SafeSearch) without being aware of doing so. Additionally, as found in other studies conducted in majority world countries (Sambasivan et al. 2018; Ahmed et al. 2019), the concept of desiring privacy had a somewhat negative valence for some participants, who said they did not need to keep their information private because they did not have anything "bad" on their devices. This could also indicate underreporting of strategies to retain privacy or concerns around privacy invasion.

In this research, we specifically focused on technology users in majority world countries, to identify beliefs and habits involving protective features. While the barriers that we identified can reasonably be extended into recommendations (e.g., low awareness of affordances→partnering with grassroots organizations or local trusted reputable sources to develop easy to use and clear resources), future research should investigate these topics in depth. It does seem likely, however, that early incorporation of user experience research with this specific population may lead to early identification of pain points to solve for, and subsequently faster and more widespread adoption of options designed for purpose.

Additionally, the scope of this study was intentionally broad, from the research questions to the features and practices we asked about. This limited how in-depth we could go about specific experiences. Future studies could take a more targeted approach and investigate perceptions of specific features (e.g., facial scanning), incorporating in situ behavioral tactics, as well as user perceptions of platform Trust & Safety responsibilities.

Although the overall sample size was relatively large, this was a purely qualitative study. Future quantitative research can be informed by this work and support findings at scale.

7 Conclusion

This exploratory research helped identify which features and settings had significant user awareness and usage, how this awareness and usage came to be, and what concerns were communicated, or not, by users. Tech companies should meet users where they are, as acknowledging those concerns, beliefs, and predispositions can help inform both future product and feature design and enforcement on existing products. We note that we intentionally sampled with a preference for users who were relatively new to internet use; however, many of these findings are similar to those seen in minority world countries, as documented in the Privacy and Security Practices section above.

Participants cited usage of long-available features and practices, with less willingness to employ strategies that are perceived as cumbersome or unreliable, even if their current practices may leave them vulnerable to increasingly sophisticated scams. The difficulty of keeping a platform safe, even in English-speaking countries, is well documented. Tech companies are scaling those operations globally, ideally in a way that is sensitive to the habits of these users (e.g., prevalence of device sharing) and adequately addresses the cultural and linguistic diversity of a global user base. Simple places to start include ensuring that education material and troubleshooting assistance are available in multiple languages. Heightening awareness and reducing misbeliefs about ways to keep oneself safe online may also be achieved by improving alternative methods of learning, such as short-form videos or commercials hosted on media sites. Nevertheless, it's true that substantial research on human behavior has indicated that such efforts may have limited success (H. Cho et al. 2023), and thus this relatively low-hanging fruit is less likely to

be effective as compared to building devices, features, and settings with an accurate assessment of user context and behaviors in mind.

Despite these challenges, these new internet users may still benefit from technological innovations. As initially noted, the efforts of keeping a user safe online fall both to the user and to the ICT companies. On the user side, rather than expecting all users to become early-adopters, a more realistic goal may be a Swiss-cheese model (Reason 1990), in which users engage a variety of settings or features, depending on their personal risk models and cost-benefit analyses. On the ICT side, ensuring that new features or settings are developed to be accessible, reliable, and convenient (which may involve partnerships between technology companies) can help facilitate and encourage adoption.

References

Abroshan, Hossein, Jan Devos, Geert Poels, and Eric Laermans. 2021. "COVID-19 and phishing: effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic." *IEEE Access* 9:121916–29. https://doi.org/10.1109/ACCESS.2021.3109091.

Acquisti, Alessandro, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, et al. 2017. "Nudges for privacy and security: Understanding and assisting users' choices online." *ACM Computing Surveys (CSUR)* 50 (3): 1–41. https://doi.org/https://doi.org/10.1145/3054926.

Ahmed, Syed Ishtiaque, Md Romael Haque, Jay Chen, and Nicola Dell. 2017. "Digital privacy challenges with shared mobile phone use in Bangladesh." *Proceedings of the ACM on Human-Computer Interaction* 1 (CSCW): 1–20. https://doi.org/https://doi.org/10.1145/3134652.

Ahmed, Syed Ishtiaque, Md Romael Haque, Irtaza Haider, Jay Chen, and Nicola Dell. 2019. "'Everyone Has Some Personal Stuff': Designing to Support Digital Privacy with Shared Mobile Phone Use in Bangladesh." In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems,* 1–13. https://doi.org/https://doi.org/10.1145/3290605.3300410.

Aissaoui, Najeh. 2021. "The digital divide: a literature review and some directions for future research in light of COVID-19." *Global Knowledge, Memory and Communication* 71 (8/9): 686–708. https://doi.org/https://doi.org/10.1108/GKMC-06-2020-0075.

Alkaldi, Nora, and Karen Renaud. 2016. "Why do people adopt, or reject, smartphone password managers?" In *Proceedings 1st European Workshop on Usable Security.* Internet Society. https://doi.org/http://dx.doi.org/10.14722/eurousec.2016.23011.

Apple. 2023. "Apple, Google, and Microsoft commit to expanded support for FIDO standard to accelerate availability of passwordless sign-ins" (May). https://www.apple.com/newsroom/2022/05/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard/.

Aruga, Kentaka, Md Monirul Islam, and Arifa Jannat. 2021. "Does Staying at Home during the COVID-19 Pandemic Help Reduce CO2 Emissions?" *Sustainability* 13 (15): 8534. https://doi.org/https://doi.org/10.3390/su13158534.

Baird, Sarah, Sarah Alheiwidi, Rebecca Dutton, Khadija Mitu, Erin Oakley, Tassew Woldehanna, and Nicola Jones. 2020. "Social isolation and disrupted privacy: Impacts of COVID-19 on adolescent girls in humanitarian contexts." *Girlhood Studies* 13 (3): 98–115. https://doi.org/https://doi.org/10.3167/ghs.2020.130308.

Barth, Susanne, and Menno D.T. De Jong. 2017. "The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior—A systematic literature review." *Telematics and Informatics* 34 (7): 1038–58. https://doi.org/https://doi.org/10.1016/j.tele.2017.04.013.

Baruh, Lemi, Ekin Secinti, and Zeynep Cemalcilar. 2017. "Online privacy concerns and privacy management: A meta-analytical review." *Journal of Communication* 67 (1): 26–53. https://doi.org/https://doi.org/10.1111/jcom.12276.

Bhagavatula, Rasekhar, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides. 2015. "Biometric authentication on iPhone and Android: Usability, perceptions, and influences on adoption." In *USEC '15: Workshop on Usable Security,* 1–10. https://ink.library.smu.edu.sg/sis_research/3967/.

Bhatlapenumarthy, Harsha. 2022. *Key Functions and Roles.* Trust & Safety Professional Association. https://www.tspa.org/curriculum/ts-curriculum/functions-roles/.

Boerman, Sophie C., Sanne Kruikemeier, and Frederik J. Zuiderveen Borgesius. 2021. "Exploring motivations for online privacy protection behavior: Insights from panel data." *Communication Research* 48 (7): 953–77. https://doi.org/https://doi.org/10.1177/0093650218800915.

Bullinger, Lindsey Rose, Jillian B. Carr, and Analisa Packham. 2021. "COVID-19 and crime: Effects of stay-at-home orders on domestic violence." *American Journal of Health Economics* 7 (3): 249–80. https://doi.org/https://doi.org/10.1086/713787.

Burrell, Jenna. 2010. "Evaluating Shared Access: social equality and the circulation of mobile phones in rural Uganda." *Journal of Computer-mediated Communication* 15 (2): 230–50. https://doi.org/https://doi.org/10.1111/j.1083-6101.2010.01518.x.

Castells, Manuel. 2002. *The Internet Galaxy: Reflections on the Internet, Business, and Society.* Oxford University Press on Demand. ISBN: 0199241538.

Chaudhry, Aliya, and Barbara Krasnoff. 2022. "How to secure your phone before attending a protest." *The Verge,* https://www.theverge.com/21276979/phone-protest-demonstration-activism-digital-how-to-security-privacy.

Cheruiyot, David, and Raul Ferrer-Conill. 2021. "Pathway outta pigeonhole? De-contextualizing majority world countries." *Media, Culture & Society* 43 (1): 189–97. https://doi.org/https://doi.org/10.1177/0163443720960907.

Cheung, Christy, Zach W.Y. Lee, and Tommy K.H. Chan. 2015. "Self-disclosure in social networking sites: the role of perceived cost, perceived benefits and social influence." *Internet Research* 25 (2). https://doi.org/https://doi.org/10.1108/IntR-09-2013-0192.

Chiu, Candy Lim, Jason Lim Chiu, and Somkiat Mansumitrchai. 2016. "Privacy, security, infrastructure and cost issues in internet banking in the Philippines: initial trust formation." *International Journal of Financial Services Management* 8 (3): 240–71. https://doi.org/10.1504/IJFSM.2016.10000998.

Cho, Geumhwan, Jun Ho Huh, Soolin Kim, Junsung Cho, Heesung Park, Yenah Lee, Konstantin Beznosov, and Hyoungshick Kim. 2020. "On the security and usability implications of providing multiple authentication choices on smartphones: the more, the better?" *ACM Transactions on Privacy and Security (TOPS)* 23 (4): 1–32. https://doi.org/https://doi.org/10.1145/3410155.

Cho, Hichang, Miriam Metzger, Sabine Trepte, and Elmie Nekmat. 2023. "A Cross-Country Study of Comparative Optimism About Privacy Risks on Social Media." *International Journal of Communication* 17:21. ISSN: 1932-8036. https://ijoc.org/index.php/ijoc/article/view/19990.

Cryst, Elena, Shelby Grossman, Jeff Hancock, Alex Stamos, and David Thiel. 2021. "Introducing the Journal of Online Trust and Safety." *Journal of Online Trust and Safety* 1 (1). https://tsjournal.org/index.php/jots/article/view/8.

Danet, Marie. 2020. "Parental concerns about their school-aged children's use of digital devices." *Journal of Child and Family Studies* 29 (10): 2890–904. https://doi.org/https://doi.org/10.1007/s10826-020-01760-y.

Das, Sanchari, Andrew Kim, Ben Jelen, Lesa Huber, and L. Jean Camp. 2020. "Non-inclusive online security: older adults' experience with two-factor authentication." In *Proceedings of the 54th Hawaii International Conference on System Sciences.* https://ssrn.com/abstract=3725888.

De Cristofaro, Emiliano, Honglu Du, Julien Freudiger, and Greg Norcie. 2013. "A comparative usability study of two-factor authentication." *arXiv preprint arXiv:1309.5344,* https://doi.org/https://doi.org/10.48550/arXiv.1309.5344.

Dienlin, Tobias, and Miriam J. Metzger. 2016. "An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample." *Journal of Computer-Mediated Communication* 21 (5): 368–83. https://doi.org/https://doi.org/10.1111/jcc4.12163.

Donner, Jonathan. 2006. "The social and economic implications of mobile telephony in Rwanda: An ownership/access typology." *Knowledge, Technology & Policy* 9:17–28. https://doi.org/https://doi.org/10.1007/s12130-006-1021-7.

Dragiewicz, Molly, Bridget Harris, Delanie Woodlock, Michael Salter, Helen Easton, Angela Lynch, Helen Campbell, Jhan Leach, and Lulu Milne. 2019. "Domestic violence and communication technology: Survivor experiences of intrusion, surveillance, and identity crime." *The Australian Communications Consumer Action Network (ACCAN),* https://doi.org/https://doi.org/10.1111/j.1745-6606.2004.tb00865.x.

Fagan, Michael, Yusuf Albayram, Mohammad Maifi Hasan Khan, and Ross Buck. 2017. "An investigation into users' considerations towards using password managers." *Human-centric Computing and Information Sciences* 7 (1): 1–20. https://doi.org/https://doi.org/10.1186/s13673-017-0093-6.

Federal Financial Institutions Examination Council. 2005. "Authentication in an internet banking environment." *FFIEC Agencies (August 2001 Guidance),* https://www.ffiec.gov/pdf/authentication_guidance.pdf.

Federal Trade Commission. 2022. "New data shows FTC received 2.8 million fraud reports from consumers in 2021," February. https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0.

Feldmann, Anja, Oliver Gasser, Franziska Lichtblau, Enric Pujol, Ingmar Poese, Christoph Dietzel, Daniel Wagner, Matthias Wichtlhuber, Juan Tapiador, Narseo Vallina-Rodriguez, et al. 2020. "The lockdown effect: Implications of the COVID-19 pandemic on internet traffic." In *Proceedings of the ACM Internet Measurement Conference,* 1–18. https://doi.org/https://doi.org/10.1145/3419394.3423658.

Frik, Alisa, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. 2022. "Users' expectations about and use of smartphone privacy and security settings." In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems,* 1–24. https://doi.org/https://doi.org/10.1145/3491102.3517504.

Gangadharan, Seeta Peña. 2017. "The downside of digital inclusion: Expectations and experiences of privacy and surveillance among marginal Internet users." *New Media & Society* 19 (4): 597–615. https://doi.org/https://doi.org/10.1177/1461444815614053.

Gao, Xianyi, Yulong Yang, Huiqing Fu, Janne Lindqvist, and Yang Wang. 2014. "Private browsing: An inquiry on usability and privacy protection." In *Proceedings of the 13th Workshop on Privacy in the Electronic Society,* 97–106. https://doi.org/https://doi.org/10.1145/2665943.2665953.

Gerber, Nina, Paul Gerber, and Melanie Volkamer. 2018. "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior." *Computers & Security* 77:226–61. https://doi.org/https://doi.org/10.1016/j.cose.2018.04.002.

Gikandi, Joyce Wangui, and Chris Bloor. 2010. "Adoption and effectiveness of electronic banking in Kenya." *Electronic Commerce Research and Applications* 9 (4): 277–82. https://doi.org/https://doi.org/10.1016/j.elerap.2009.12.003.

Gilbert, David. 2020. "Hate Speech on Facebook is Pushing Ethiopia Dangerously Close to a Genocide." *Vice* 14 (September). https://www.vice.com/en/article/xg897a/hate-speech-on-facebook-is-pushing-ethiopia-dangerously-close-to-a-genocide.

Hanibuchi, Tomoya, Naoto Yabe, and Tomoki Nakaya. 2021. "Who is staying home and who is not? Demographic, socioeconomic, and geographic differences in time spent outside the home during the COVID-19 outbreak in Japan." *Preventive Medicine Reports* 21:101306. https://doi.org/10.1016/j.pmedr.2020.101306.

Henry, Nicola, Asher Flynn, and Anastasia Powell. 2020. "Technology-facilitated domestic and sexual violence: A review." *Violence against Women* 26 (15-16): 1828–54. https://doi.org/https://doi.org/10.1177/1077801219875821.

Hill, David, Nusheen Ameenuddin, Yolanda Linda Reid Chassiakos, Corinn Cross, Jeffrey Hutchinson, Alanna Levine, Rhea Boyd, Robert Mendelson, Megan Moreno, Wendy Sue Swanson, et al. 2016. "Media and young minds." *Pediatrics* 138 (5). https://doi.org/10.1542/peds.2016-2591.

Ibrahim, Amal. 2019. "Cyberactivism and Empowerment: Egyptian Women's Advocacy to Combat Sexual Harassment." *Social media and society* 8:167–86. https://api.semanticscholar.org/CorpusID:212782952.

Ibtasam, Samia, Lubna Razaq, Maryam Ayub, Jennifer R. Webster, Syed Ishtiaque Ahmed, and Richard Anderson. 2019. "'My cousin bought the phone for me. I never go to mobile shops.": The Role of Family in Women's Technological Inclusion in Islamic Culture." *Proceedings of the ACM on Human-Computer Interaction* 3 (CSCW): 1–33. https://doi.org/https://doi.org/10.1145/3359148.

ICO. 2020. "Age appropriate design: a code of practice for online services." https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/.

Insurance Information Institute. 2022. *Facts + Statistics: Identity theft and cybercrime.* https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.

Jain, Anil K., and Ajay Kumar. 2012. "Biometric recognition: an overview." In *Second Generation Biometrics: The Ethical, Legal and Social Context,* 49–79. Springer. ISBN: 9789400738911.

James, Jeffrey. 2021. "Confronting the scarcity of digital skills among the poor in developing countries." *Development Policy Review* 39 (2): 324–39. https://doi.org/https://doi.org/10.1111/dpr.12479.

Karlson, Amy K., A.J. Bernheim Brush, and Stuart Schechter. 2009. "Can I borrow your phone? Understanding concerns when sharing mobile phones." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 1647–50. https://doi.org/https://doi.org/10.1145/1518701.1518953.

Kelley, Patrick Gage, Lorrie Faith Cranor, and Norman Sadeh. 2013. "Privacy as part of the app decision-making process." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 3393–402. https://doi.org/https://doi.org/10.1145/2470654.2466466.

Kikerpill, Kristjan, and Andra Siibak. 2021. "Abusing the COVID-19 Pan(dem)ic: A Perfect Storm for Online scams." In *COVID-19 in International Media,* 249–58. Routledge. https://doi.org/10.4324/9781003181705-25.

Koh, David. 2020. "COVID-19 lockdowns throughout the world." *Occupational Medicine* 70 (5): 322–22. https://doi.org/10.1093/occmed/kqaa073.

Kokolakis, Spyros. 2017. "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon." *Computers & Security* 64:122–34. https://doi.org/https://doi.org/10.1016/j.cose.2015.07.002.

Kostka, Genia, Léa Steinacker, and Miriam Meckel. 2022. "Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology." *Government Information Quarterly,* 101761. https://doi.org/https://doi.org/10.1016/j.giq.2022.101761.

Kumar, Priya, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2017. "'No Telling Passcodes Out Because They're Private': Understanding Children's Mental Models of Privacy and Security Online." *Proceedings of the ACM on Human-Computer Interaction* 1 (CSCW): 1–21. https://doi.org/https://doi.org/10.1145/3134699.

Kumaran, Neil. 2019. *Spam does not bring us joy—ridding Gmail of 100 million more spam messages with TensorFlow.* Technical report. Google Cloud. https://workspace.google.com/blog/product-announcements/ridding-gmail-of-100-million-more-spam-messages-with-tensorflow.

Kumaran, Neil, and Sam Lugani. 2020. *Protecting businesses against cyber threats during COVID-19 and beyond.* Technical report. Google Cloud. https://cloud.google.com/blog/products/%20identity-security/protecting-against-cyber-threats-duringcovid-19-and-beyond.

Lallie, Harjinder Singh, Lynsay A. Shepherd, Jason R.C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. 2021. "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic." *Computers & Security* 105:102248. https://doi.org/https://doi.org/10.1016/j.cose.2021.102248.

Lichtenstein, Bronwen, and Ida M. Johnson. 2009. "Older African American women and barriers to reporting domestic violence to law enforcement in the rural Deep South." *Women & Criminal Justice* 19 (4): 286–305. https://doi.org/https://doi.org/10.1080/08974450903224329.

Lyles, Taylor. 2022. "Google Updates Pixel 4 with 'eyes open' fix for face unlock." *The Verge* (April). https://www.theverge.com/2020/4/6/21211230/google-update-pixel-4-eyes-open-fix-face-unlock.

Madrid Akpovo, Samara, Lydiah Nganga, and Diptee Acharya. 2018. "Minority-world pre-service teachers' understanding of contextually appropriate practice while working in majority-world early childhood contexts." *Journal of Research in Childhood Education* 32 (2): 202–18. https://doi.org/https://doi.org/10.1080/02568543.2017.1419321.

Masur, Philipp K. 2018. *Situational Privacy and Self-disclosure: Communication Processes in Online Environments.* Springer. ISBN: 978-3-319-78884-5.

Matthews, Tara, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. "'She'll just grab any device that's closer': A Study of Everyday Device & Account Sharing in Households." In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems,* 5921–32. https://doi.org/https://doi.org/10.1145/2858036.2858051.

Korn, Jennifer. 2023. "Meta rolls out paid verification option for Facebook and Instagram users in US" (March 17, 2023). https://www.cnn.com/2023/03/17/tech/meta-verified-us-launch/index.html.

Milne, George R., Andrew J. Rohm, and Shalini Bahl. 2004. "Consumers' protection of online privacy and identity." *Journal of Consumer Affairs* 38 (2): 217–32. https://doi.org/https://doi.org/10.1111/j.1745-6606.2004.tb00865.x.

Min, Jinyoung, and Byoungsoo Kim. 2015. "How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost." *Journal of the Association for Information Science and Technology* 66 (4): 839–57. https://doi.org/https://doi.org/10.1002/asi.23206.

Nolte, Julia, Yaniv Hanoch, Stacey Wood, and David Hengerer. 2021. "Susceptibility to COVID-19 Scams: The Roles of Age, Individual Difference Measures, and Scam-Related Perceptions." *Frontiers in Psychology* 12:789883–83. https://doi.org/https://doi.org/10.3389/fpsyg.2021.789883.

Normington, Mark. 2022. *Briefing October 2022: TikTok AND Facebook Fail To Detect Election Disinformation in the US.* Technical report. Global Witness. https://doi.org/20.500.12592/m47690..

Oduor, Erick, Carman Neustaedter, Tejinder K. Judge, Kate Hennessy, Carolyn Pang, and Serena Hillman. 2014. "How technology supports family communication in rural, suburban, and urban Kenya." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 2705–14. https://doi.org/https://doi.org/10.1145/2556288.2557277.

Oesch, Sean, Scott Ruoti, James Simmons, and Anuj Gautam. 2022. "'It Basically Started Using Me:' An Observational Study of Password Manager Usage." In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems,* 1–23. https://doi.org/https://doi.org/10.1145/3491102.3517534.

Oloyede, Abdulkarim A., Nasir Faruk, and Wasiu O. Raji. 2022. "COVID-19 lockdown and remote attendance teaching in developing countries: A review of some online pedagogical resources." *African Journal of Science, Technology, Innovation and Development* 14 (3): 678–96. https://doi.org/https://doi.org/10.1080/20421338.2021.1889768.

Pearman, Sarah, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2019. "Why people (don't) use password managers effectively." In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019),* 319–38. Santa Clara, CA: USENIX Association. ISBN: 978-1-939133-05-2. https://www.usenix.org/conference/soups2019/presentation/pearman.

Petrosyan, Ani. 2021. *Percentage of global population accessing the internet from 2005 to 2021, by market maturity.* https://www.statista.com/statistics/209096/share-of-internet-users-in-the-total-world-population-since-2006/.

Ponciano, Jonathan. 2022. "The World's Largest Tech Companies in 2022: Apple Still Dominates as Brutal Market Selloff Wipes Trillions in Market Value." *Forbes Magazine,* https://www.forbes.com/sites/jonathanponciano/2022/05/12/the-worlds-largest-technology-companies-in-2022-apple-still-dominates-as-brutal-market-selloff-wipes-trillions-in-market-value/?sh=3ddbc6234488.

Powell, Mary Ann, Anne Graham, Nicola J. Taylor, Sallie Newell, and Robyn Fitzgerald. 2011. "Building capacity for ethical research with children and young people: An international research project to examine the ethical issues and challenges in undertaking research with and for children in different majority and minority world contexts." *Childwatch International Research Network,* https://www.researchgate.net/publication/254664116_Building_Capacity_for_Ethical_Research_with_Children_and_Young_People_An_International_Research_Project_to_Examine_the_Ethical_Issues_and_Challenges_in_Undertaking_Research_With_and_For_Children_in_Di.

Pratama, Ahmad R., and Firman M. Firmansyah. 2021. "Until you have something to lose! Loss aversion and two-factor authentication adoption." *Applied Computing and Informatics,* no. ahead-of-print, https://doi.org/https://doi.org/10.1108/ACI-12-2020-0156.

Ragnedda, Massimo, and Glenn W. Muschert. 2017. *Theorizing Digital Divides.* Routledge. https://doi.org/https://doi.org/10.4324/9781315455334.

Rainie, Lee, Sara Kiesler, Ruogu Kang, Mary Madden, Maeve Duggan, Stephanie Brown, and Laura Dabbish. 2013. "Anonymity, privacy, and security online." *Pew Research Center* 5. http://pewinternet.org/Reports/2013/Anonymity-online.aspx.

Reason, James. 1990. *Human Error.* Cambridge University Press. https://doi.org/10.1017/CBO9781139062367.

Reserve Bank of India. 2021. *Master Direction on Digital Payment Security Controls.* https://www.rbi.org.in/scripts/FS_Notification.aspx?Id=12032&fn=2&Mode=0#14.

Reznik, Maksim. 2012. "Identity theft on social networking sites: Developing issues of internet impersonation." *Touro Law Review* 29:455. https://digitalcommons.tourolaw.edu/lawreview/vol29/iss2/12?utm_source=digitalcommons.tourolaw.edu%2Flawreview%2Fvol29%2Fiss2%2F12&utm_medium=PDF&utm_campaign=PDFCoverPages.

Rossini, Carolina, Francisco Brito Cruz, and Danilo Doneda. 2015. *The strengths and weaknesses of the Brazilian Internet Bill of Rights: Examining a Human Rights Framework for the Internet.* Technical report. Global Commission on Internet Governance. https://www.cigionline.org/publications/strengths-and-weaknesses-brazilian-internet-bill-rights-examining-human-rights/.

Sambasivan, Nithya, Nova Ahmed, Amna Batool, Elie Bursztein, Elizabeth Churchill, Laura Sanely Gaytan-Lugo, Tara Matthews, David Nemar, Kurt Thomas, and Sunny Consolvo. 2019. "Toward Gender-Equitable Privacy and Security in South Asia." *IEEE Security & Privacy* 17 (4): 71–77. https://doi.org/10.1109/MSEC.2019.2912727.

Sambasivan, Nithya, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. 2018. ""Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia." In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018),* 127–42. Baltimore, MD: USENIX Association, August. ISBN: 978-1-939133-10-6. https://www.usenix.org/conference/soups2018/presentation/sambasivan.

Smith, Aaron. 2019. "More than half of US adults trust law enforcement to use facial recognition responsibly." *Pew Research Center,* https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/.

Souza, Carlos Affonso Pereira de, and Beatriz Laus Marinho Nunes. 2022. "Brazilian Internet Bill of Rights: The Five Roles of Freedom of Expression." In *Personality and Data Protection Rights on the Internet. Ius Gentium: Comparative Perspectives on Law and Justice,* edited by Marion Albers and Wolfgang Sarlet Sarlet, 213–39. Springer. https://doi.org/https://doi.org/10.1007/978-3-030-90331-2_9.

Spencer, Chelsea, Allen Mallory, Michelle Toews, Sandra Stith, and Leila Wood. 2017. "Why sexual assault survivors do not report to universities: A feminist analysis." *Family Relations* 66 (1): 166–79. https://doi.org/https://doi.org/10.1111/fare.12241.

Statista Research Department. 2023. "Forecasted number of digital banking users in the United States from 2021 to 2025 (in millions)," May 2, 2023. https://www.statista.com/statistics/1285962/digital-banking-users-usa/.

Steenson, Molly Wright, and Jonathan Donner. 2017. "Beyond the personal and private: Modes of mobile phone sharing in urban India." In *The Reconstruction of Space and Time,* 231–50. Routledge. ISBN: 9781315134499.

Stock, Jürgen. 2020. "INTERPOL report shows alarming rate of cyberattacks during COVID-19." *Interpol,* https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

Tazi, Maha. 2021. "The Arab Spring and Women's (Cyber) activism: 'Fourth Wave Democracy in the Making?' Case Study of Egypt, Tunisia, and Morocco." *Journal of International Women's Studies* 22 (9): 298–315. https://vc.bridgew.edu/jiws/vol22/iss9/20.

Ticona, Julia. 2022. "Red flags, sob stories, and scams: The contested meaning of governance on carework labor platforms." *New Media & Society* 24 (7): 1548–66. https://doi.org/https://doi.org/10.1177/14614448221099233.

Tidy, Joe. 2020. "Google blocking 18m coronavirus scam emails every day." *BBC* (April). https://www.bbc.com/news/technology-52319093.

Trepte, Sabine, Doris Teutsch, Philipp K. Masur, Carolin Eicher, Mona Fischer, Alisa Hennhöfer, and Fabienne Lind. 2015. "Do people know about privacy and data protection strategies? Towards the 'Online Privacy Literacy Scale'(OPLIS)." In *Law, Governance, and technology series: Vol. 20. Reforming European Data Protection Law,* edited by Serge Gutwirth, Ronald Leenes, and Paul de Hert, 333–65. Springer. https://doi.org/https://doi.org/10.1007/978-94-017-9385-8_14.

Twitter Help. 2023. "How to get the blue checkmark on Twitter." https://help.twitter.com/en/managing-your-account/about-twitter-verified-accounts.

Ulqinaku, Enis, Hala Assal, Abdou AbdelRahman, Sonia Chiasson, and Srdjan Capkun. 2021. "Is Real-time Phishing Eliminated with FIDO? Social Engineering Downgrade Attacks against FIDO Protocols." In *Proceedings of the 30th USENIX Security Symposium (USENIX Security 21),* 3811–28. USENIX Association. https://www.usenix.org/conference/usenixsecurity21/presentation/ulqinaku.

Van Dijk, Jan A.G.M. 2006. "Digital divide research, achievements and shortcomings." *Poetics* 34 (4-5): 221–35. https://doi.org/https://doi.org/10.1016/j.poetic.2006.05.004.

Wang, Chun, Steve T.K. Jan, Hang Hu, Douglas Bossart, and Gang Wang. 2018. "The next domino to fall: Empirical analysis of user passwords across online services." In *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy,* 196–203. https://doi.org/https://doi.org/10.1145/3176258.3176332.

Wiederhold, Brenda K. 2020. "Children's screen time during the COVID-19 pandemic: boundaries and etiquette." *Cyberpsychology, Behavior, and Social Networking* 23 (6): 359–60. https://doi.org/10.1089/cyber.2020.29185.bkw.

Wolf, Flynn, Ravi Kuber, and Adam J Aviv. 2019. "'Pretty Close to a Must-Have': Balancing Usability Desire and Security Concern in Biometric Adoption." In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems,* 1–12. https://doi.org/https://doi.org/10.1145/3290605.3300381.

Wood, Stacey, David Hengerer, and Yaniv Hanoch. 2022. "Scams in the Time of COVID-19: Pandemic Trends in Scams and Fraud." In *A Fresh Look at Fraud,* 42–57. Routledge.

Woodlock, Delanie. 2017. "The abuse of technology in domestic violence and stalking." *Violence against Women* 23 (5): 584–602. https://doi.org/https://doi.org/10.1177/1077801216646277.

Woodward, J.D. 1997. "Biometrics: privacy's foe or privacy's friend?" *Proceedings of the IEEE* 85 (9): 1480–92. https://doi.org/10.1109/5.628723.

Wu, Yuxi, Panya Gupta, Miranda Wei, Yasemin Acar, Sascha Fahl, and Blase Ur. 2018. "Your secrets are safe: How browsers' explanations impact misconceptions about private browsing mode." In *Proceedings of the 2018 World Wide Web Conference,* 217–26. https://doi.org/https://doi.org/10.1145/3178876.3186088.

Zou, Yixin, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. 2020. "Examining the adoption and abandonment of security, privacy, and identity theft protection practices." In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems,* 1–15. https://doi.org/https://doi.org/10.1145/3313831.3376570.

Zuboff, Shoshana. 2015. "Big other: surveillance capitalism and the prospects of an information civilization." *Journal of Information Technology* 30 (1): 75–89. https://doi.org/https://doi.org/10.1057/jit.2015.5.

Authors

Rebecca Umbach is a Senior UX Researcher on the Trust & Safety Research Team at Google in San Francisco.

(rumbach@google.com)

Anubha Singh is a UX Researcher on the Trust & Safety Research Team at Google in Sunnyvale.

Ashley Marie Walker is a Senior UX Researcher on the Trust & Safety Research Team at Google in New York.

Acknowledgements

We'd like to thank our participants for sharing their experiences. Without their candor, this research wouldn't have been possible.

Keywords

at-risk users; online harm; digital safety; vulnerable populations; new internet users; majority world users