EDIT
EVIDENCE FOR DIGITAL TRANSFORMATION Consortium

Gates Foundation

Measuring Digital Harms in Low and Middle-Income Countries

A guide for inclusive research and design

2x Digital

UNIVERSITY OF CAPE TOWN
IYUNIVESITHI YASEKAPA • UNIVERSITEIT VAN KAAPSTAD

School of Public Health
Departement Openbare Gesondheid
Isikolo Sempilo Yoluntu
UNIVERSITY OF CAPE TOWN

YORK U

JOHNS HOPKINS
BLOOMBERG SCHOOL of PUBLIC HEALTH

Measuring Digital Harms in Low and Middle-Income Countries

A guide for inclusive research and design

Table of Contents

Acknowledgements

This Toolkit was developed by a consortium of partners led by the University of Cape Town's School of Public Health, consisting of the University of Cape Town, the Johns Hopkins Bloomberg School of Public Health, York University, and 2X Digital. The Toolkit was developed with support from the Gates Foundation. Authors included Amnesty LeFevre, Angelica Panieri, Loveness Kimaro, Kerry Scott, Osama Ummer, Anjora Sarangi, Sara Chamberlain, Mayank Date, and Diwakar Mohan.

The Toolkit leverages technical inputs from partners obtained through individual consultations, online webinars hosted by the GSMA's Knowledge Hub, and workshops conducted in New Delhi in 2023, 2024 and 2025. The content represents original information and information that has been adapted through cognitive testing in India, Kenya and Nigeria. We thank DevSol Research Consultant Private Limited for conducting the cognitive interviews for UCT in India, and Ipsos for conducting the cognitive interviews for UCT in Kenya and Nigeria.

We thank the following organizations for providing access to their original surveys: BBC Media Action, European Commission, EUROSTAT, Global Kids Online, the GSMA, ICF Macro, International Institute of Population Sciences (IIPS), International Telecommunication Union (ITU), Kilkari Impact Evaluation Team, National Institutes for Statistics, PEW Research Center, Philippine Survey and Research Organization, Research ICT Africa, SurveyMETER, TRUSTe, UNICEF, United Nations Capital Development Fund, University of Oxford, and the World Bank.

We additionally wish to thank Dan Harder for graphic design.

1.0 Overview

1.1 Introduction

The spread of digital technologies, including mobile phones, brings new opportunities—but also an increasing potential for technology-related harms [1, 2]. These risks manifest in multiple forms: online safety concerns such as cyberbullying, harassment, fraud, and exposure to harmful or misleading content [3, 4]; threats to privacy and data protection due to widespread data collection, surveillance, and misuse of personal information [5]; as well as health-related concerns including excessive screen time, technology overuse, and negative impacts on mental health and social well-being [6].

Despite these growing risks, available evidence remains limited and largely concentrated in high-resource settings. What data exist suggest that women may be disproportionately affected and at greater risk of harm [6-8]. In low- and middle-income countries, where women continue to face significant barriers to technology access and use, the gendered dimensions of digital inequality further compound these vulnerabilities [9].

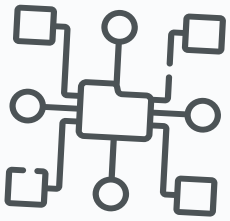
In some contexts, gender norms may restrict women's use of mobile phones–both in scope and frequency–partly due to fears of reputational harm or exposure to gendered digital risks [10]. In other contexts, while women's use of phones is not restricted, patriarchal gender norms result in women experiencing gendered digital harms, particularly misogynistic harassment online [10]. However, since the use of digital technologies transcends gender boundaries, men, including adolescent boys, may also be vulnerable to various technology-related harms [11].

Robust, contextually relevant data on the harms associated with technology use are critical for improving visibility, enabling evidence-based decision-making, and shaping effective mitigation strategies through program and policy design. Broadly, five common types of data are used to assess technology-related harms: (1) survey data generated through large-scale, population-based surveys; (2) survey data collected through online platforms, which are often faster and lower-cost but may suffer from representativeness challenges; (3) administrative or service-based data, such as records from helplines, schools, or health services; (4) secondary analyses of digital trace data, including the application of machine learning and natural language processing techniques to scrape and analyze social media content; and (5) qualitative data, including in-depth interviews, focus group discussions, and participatory methods that capture lived experiences and contextual dynamics [12]. Among these, population-based surveys offer the greatest potential for robust, comparable, and representative measurement of the prevalence, modality, impact, and response to harms, though they require significant resources and careful ethical safeguards [13]. This methodology ensures broader reach, supports inclusion of individuals with limited literacy or digital access, and enables the collection of more reliable and representative data on the prevalence, nature, and impacts of digital harms.

1.2 Toolkit aims

This toolkit aims to support the inclusive and gender-intentional measurement of harms associated with technology use (hereafter referred to as "digital harms") in low- and middle-income countries. The toolkit outlines approaches for measuring digital harms at the population level, with a particular emphasis on quantitative, in-person surveys facilitated by trained enumerators.

1.3 Toolkit structure



The survey questions in this toolkit are categorised into three categories, as seen in table 1. Each domain includes a set of recommended quantitative survey questions that can be used to measure mobile phone access in low and middle-income countries. Many of these questions were drawn from global surveys identified in the literature and subsequently enhanced through cognitive interviews in India, Kenya and Nigeria.

Section 1: Conceptual foundations

We begin by reviewing key terminology related to digital harms and propose six typologies of harms:

1. Digital violence
2. Misinformation, disinformation, and malinformation
3. Digital fraud
4. Violations of privacy and data protection
5. Physical and mental health impacts of technology use
6. Biases in artificial intelligence (AI) and algorithms

Section 2: Survey question development and framework

We describe the process of question development and refinement, introduce a measurement framework, and highlight key considerations for the responsible measurement of harms through structured quantitative surveys. These recommendations are informed by a review of existing survey instruments and cognitive testing conducted in India, Nigeria, and Kenya.

Section 3: Measurement at the individual level

We provide an overview of metrics for measuring digital harms at the individual level, organized around five of the six core typologies. We have not included metrics for measuring biases in AI and algorithms because these are challenging to measure through population-based surveys and are better measured by analysing large sets of AI outputs and metadata, and by domain experts reviewing AI outputs for fairness, accuracy, and harmful patterns.

Annexes

The Toolkit concludes with a set of annexes, including supplementary materials, detailed survey question examples, translation guidance, and resources for implementation.

1.4 Limitations

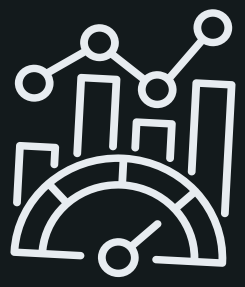
Measuring harms is inherently complex and must be tailored to the specific context, considering both the data needs for program design and decision-making, and what can be measured ethically and responsibly without placing undue burden on respondents.

This toolkit presents examples of harms that may be appropriate to measure, while acknowledging that not all harms can be captured through structured, quantitative surveys. The included questions are designed for administration through in-person surveys at both the population and individual levels. As a result, certain digital harm typologies—such as AI bias and some types of digital fraud such as ransomware attacks and malware deployment are not covered, as they are difficult to measure through population-level surveys. These are better assessed through secondary analyses of AI outputs, metadata, or qualitative interviews with technical experts who can provide more nuanced insights on the harms encountered.

The toolkit has also been designed for use in low-resource settings. Accordingly, response options—such as the medium through which the harm was experienced—and some terminology should be adapted to fit the local context of implementation.

Finally, while the toolkit addresses certain physical and mental health impacts of technology use, it does not include questions on self-injurious thoughts and behaviors (e.g., suicidal ideation or attempts). Such questions are best suited to contexts where individuals can access immediate care and support such as in a health care facility.

2.0 Defining and measuring digital harms



2.1 What are digital harms?

Digital harms are the negative outcomes associated with use of digital technologies [15]. These can be direct or indirect, intentional or unintentional, and they cut across social, psychological, economic, and political dimensions. Digital harms may be broken down into six types (Table 1).

Table 1. Defining types of digital harms

Type of harm	Definition	Questions covered in the Toolkit
Digital Violence	Digital violence encompasses both online and offline technology-facilitated violence: **Online technology-facilitated violence** refers to harmful behaviors or actions carried out through digital technologies, online platforms, or electronic communication tools, with the intent to intimidate, control, harass, exploit, or otherwise cause harm [8]. **Offline technology-facilitated violence** refers to emotional or physical abuse that is triggered, escalated, or justified by the use of digital technologies.	**Online technology facilitated violence**: **Online abuse and harassment** such as cyberstalking, cyberbullying and online hate speech. **Sexual digital violence**, including revenge porn, upskirting, sexting coercion, sextortion, deepfakes, and cyberflashing. **Doxxing.** **Offline technology-facilitated violence**: Emotional abuse related to phone use, Physical violence related to phone use.
Misinformation, disinformation, malinformation	A range of ways in which sharing information causes harm, intentionally or unintentionally [15].	**False information**
Digital fraud	Loss of money through deceit, including via mobile (cellular) networks (e.g., calls, SMS) and the internet.	Online shopping scams, Romance scams, Mobile money fraud, Identity theft via phishing Business email compromise.
Violations of privacy and data protection	Harms from misuse of data, repurposing personal information, unwanted data retention, continued sharing of personal data, lack of data accuracy, or transparency [16].	Identify theft Surveillance and tracking Data breaches Consent and autonomy violations Data misuse Data profiling and discrimination Rights to erasure violations.

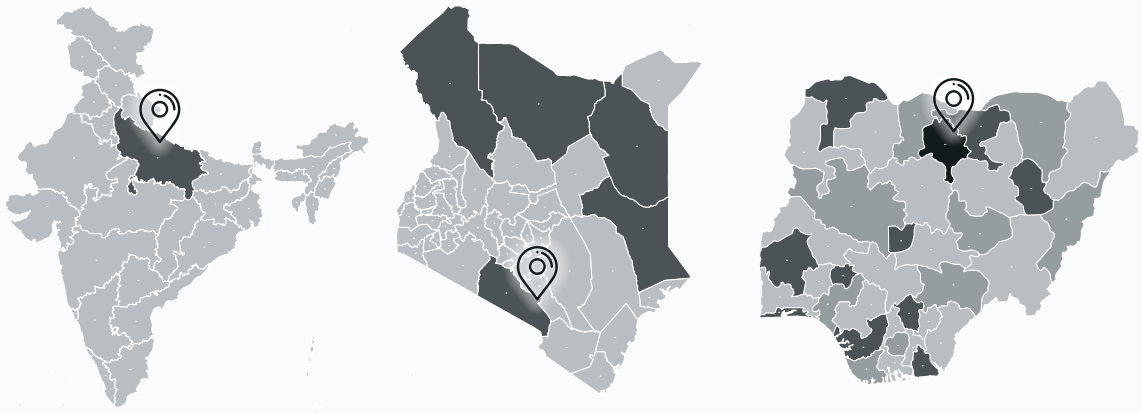
Type of harm	Definition	Questions covered in the Toolkit
Physical and mental health impact of technology use	Negative impacts on individuals' wellbeing (physical and mental) associated with frequent use of digital technology [17].	**Physical impacts:** Sleep disturbances, visual disturbances, musculoskeletal complaints, headaches. **Mental health impacts:** Anxiety, social media addiction or problematic social media use, depression, body image and disordered eating outcomes, self-injurious thoughts and behaviors.
Biases in artificial intelligence (AI) and algorithms.	Systematic and unfair discrimination against certain individuals or groups, arising from skewed data, flawed algorithms, or biased human decisions embedded in AI systems, leading to harmful or unequal outcomes	Metrics for measuring biases in AI are not included because they are challenging to accurately measure through population-based surveys and are better measured by analysing large sets of AI outputs and metadata, and by domain experts reviewing AI outputs for fairness, accuracy, and harmful patterns.

2.2 Measuring harms through structured quantitative surveys

2.2.1 Process for identifying harms related questions

Quantitative survey questions on digital harms were identified through a scoping review of the literature, including population-based surveys, and further refined through a series of expert consultations held in India and virtually between 2023 and 2025. A subsample of questions underwent cognitive testing in India, Kenya, and Nigeria during 2023–2024 [18, 19]. Based on the findings from these interviews, the content and translations of the questions were iteratively refined to improve clarity, cultural relevance, and validity.

Figure 1. Number of cognitive interviews completed across India, Kenya and Nigeria



India; Hindi (n=101 CIs)
Janpur
Bareilly
Budan
(Uttar Pradesh)

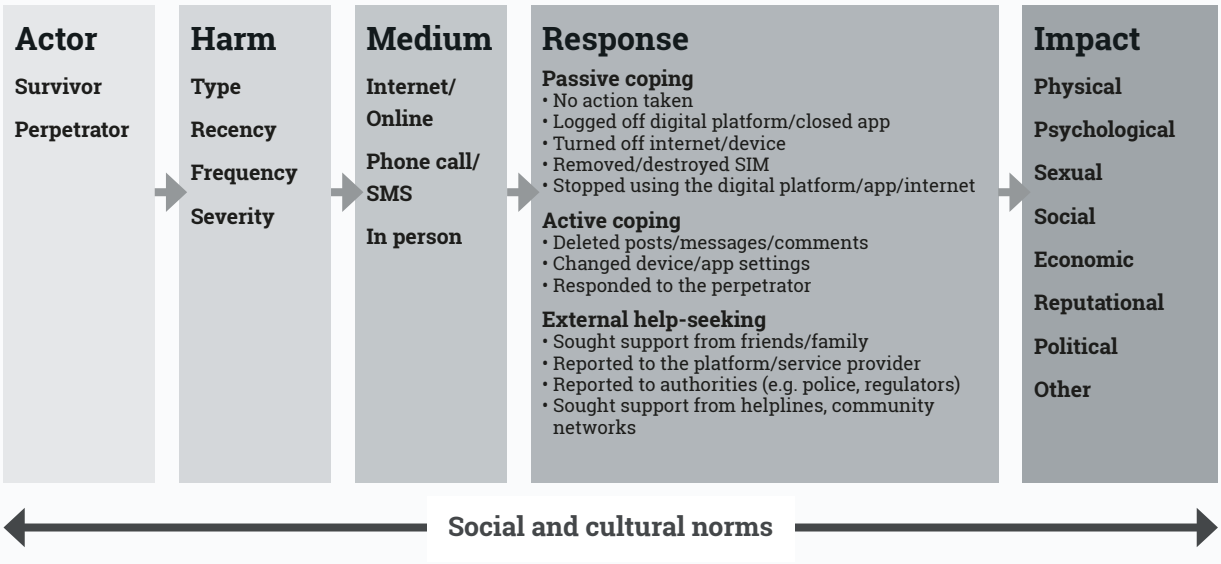
Kenya; Kiswahili (n=90CIs)
Nairobi
Kajiado
Makueni
Murang'a

Nigeria; Hausa (n=90CIs)
Kano City
North Kano
Central Kano
South Kano

2.2.2 Proposed framework for measuring digital harms

Figure 3 builds off prior frameworks developed by the International Center for Research on Women (ICRW) in 2018 [20] for the measurement of technology facilitated gender-based violence. We have adapted this approach and recommend applying it more broadly in population-based quantitative surveys to measure five of the six categories of digital harms shown in Figure 1.

Figure 2. Measuring harms related to technology use in population-based quantitative surveys. Adapted from ICRW 2018-2019 [21].



This framework illustrates the pathway from harm to impact, highlighting how social and cultural norms shape each stage of the process. It underscores that experiences of digital harms are not only mediated by the type of harm and medium through which it occurs, but also by survivors' responses and the resulting impacts across physical, psychological, social, economic, and political dimensions. In practice, most quantitative surveys seek to measure harms primarily from the perspective of the survivor—defined here as the person who directly experiences the harm.

2.2.3 Key considerations for digital harms measurement

Harms measurement requires careful consideration of the ethical and safety ramifications for both respondents and enumerators. Building off the WHO's recommendations for research on violence against women [21] and those elsewhere in the literature [22, 23], we outline the following key considerations for the ethical and safe measurement of harms.

Prioritize the safety of both respondents and the research team

To ensure the safety of both respondents and the research team, the risks associated with measuring digital harms should be considered and mitigation measures put in place before data collection begins. For specialized surveys focused specifically on digital harms, consider establishing a Data Safety and Monitoring Board (DSMB) to provide independent oversight of risk management, incident reporting, and response strategies. Safety protocols should also outline procedures for handling urgent situations, including when a participant discloses imminent risk of self-harm or violence. Finally, research teams must plan for the safety of enumerators, who may face secondary traum a when engaging with sensitive topics during the research period. Enumerators much also be protected from digital harms themselves while conducting the survey research. Ensuring that all enumerators provide only a central

institutional phone number and email address to respondents (rather than any personal contact information) will protect them from harassment. Enumerators should also be trained to refuse to look at participant phones to ensure they are not exposed to inappropriate or disturbing digital content, for example, if a participant offers to show them an image that was sent to them in order to explain an instance of harassment, the enumerator must be trained to explain that this is not permitted by their research organization.

Ensure confidentiality

Protecting confidentiality is essential to safeguarding respondents and to maintaining the integrity and quality of data collected. This requires strict data protection protocols, such as encrypted data storage, anonymization of responses, and clear limits on who has access to identifiable information. Researchers should anticipate digital-specific risks, including unauthorized access to devices used for surveys, and implement safeguards accordingly. Respondents should be informed—using clear and accessible language—about how their data will be protected, how it will be used, and under what circumstances, if any, disclosure may be required (e.g., in the case of imminent harm). Maintaining trust through robust confidentiality practices not only reduces risks to participants, in accordance with principles of ethical research practice, but also strengthens the reliability of survey findings.

Select and support the research team carefully

All research team members should be carefully selected and receive specialized training and ongoing support. Given the sensitivity of digital harms research, recruitment should prioritize staff with relevant experience, cultural competence, and demonstrated commitment to ethical research practices. If surveys ask about specifically gendered aspects of digital harm, female enumerators should interview female respondents and male enumerators should interview male respondents to build trust, reduce discomfort, and encourage more open disclosure of sensitive experiences.

Specialized training should extend beyond technical survey skills to include trauma-informed approaches, strategies for responding to distress, and guidance on safeguarding both participants and enumerators from online and offline risks. Continuous support mechanisms—such as regular supervision, structured debriefings, and access to psychosocial resources—should be built into the project design to help prevent secondary trauma, compassion fatigue, and burnout among research staff.

In addition, teams should establish clear codes of conduct, confidentiality agreements, and accountability mechanisms to reinforce professional standards and ethical responsibilities. Creating a supportive and well-prepared team environment is essential not only to protecting respondents but also to ensuring the integrity and quality of the research process.

Establish referral systems and sources of support for victims requesting assistance. Where few resources exist, it may be necessary for the study to create short-term support mechanisms.

The type and severity of digital harms experienced by survey participants may necessitate additional medical and/or psychological support for affected individuals. While the survey will adhere to core research principles—such as safeguarding the confidentiality of participants' information—there remains an ethical obligation to ensure that victims of digital harms, particularly those involving physical violence, are provided with appropriate support [21]. To

fulfill this responsibility, the research team should identify and establish connections with existing resources and facilities that assist victims of violence. In some contexts, these resources may not exist or be possible to establish. In which case, it may not be feasible to conduct the survey outright or measure all typologies of harms. In the event such system can be assured, enumerators should work in close coordination with both the research team and local authorities to facilitate referrals for participants requiring further medical care and/or psychological support. In cases where victims face barriers in accessing services—such as transportation or financial constraints—the research team should arrange escorted referrals. However, in doing so, the team must take care not to disclose a participant's involvement in the survey or share any information collected with service providers.

Measuring and monitoring harm related to the research should be incorporated into safety protocols.

Researchers have an ethical responsibility to monitor and assess harms, or potential harms, that may arise during the course of a study, and to evaluate whether research participation results in any such experiences. The research team should anticipate and define a process for documenting, investigating and responding to safety issues and incidents. Any potential harm that comes to the attention of researchers should be documented. A case-by-case assessment will be required to determine whether the incident is related to the study and what, if any, follow-up actions are appropriate.

Researchers and donors have an ethical obligation to help ensure that their findings are properly interpreted and used to advance policy and intervention development.

To support this process, WHO recommends that local stakeholders be engaged from the outset to foster context specific planning. The strength of evidence derived from survey data should be critically evaluated, while also identifying any additional data required to guide decisions on the availability and design of effective interventions for the target population [21].

2.2.4 General principles for survey design

Surveys with mixed or low literate populations must be facilitated (rather than self-administered)

In deciding how to administer a structured survey, implementers should consider the population's age, education and literacy, time available for the survey, and specific survey needs. Among high literacy populations, respondents can be asked to self-administer the survey but among populations with mixed or low literacy, surveys should be facilitated by an enumerator.

Use simple and easy to understand language, including contextually appropriate terms

Prioritize words that are widely used and understood. Well-known local terms for subordinate items, such as brand names, are easier for respondents to understand than global hypernyms (terms for the entire category). For example, asking about harms faced on "Facebook, Instagram, Twitter etc." is clearer to respondents than asking about harms faced on "social media platforms".

Measure one construct at a time

Questions that ask about multiple constructs result in inconsistent and unclear measurement. Questions should measure just one construct at a time.

Keep sentences short and avoid unnecessary qualifiers and clauses

Questions with multiple clauses increase the cognitive burden placed on respondents and can lead to confusion. Remove non-essential clauses and qualifiers.

For administered surveys, use the "question answer" format rather than "statement response" format.

Instead of having an enumerator read the statement "I have [experienced X]" and inviting the respondent to respond "agree" or "disagree", have the enumerator ask "Have you ever [experienced X]?" and have the respondent answer yes or no.)

Use simple response options and short (three-point) Likert scales

Gradients of feeling or intensity of agreement/disagreement do not resonate in some populations. Thus, in some populations, "strongly agree" or "somewhat agree" are not understood as distinct categories. Three-point scales work across populations.

Phrase each question to be stand-alone and avoid stem and leaf style questions.

Each question should stand alone. Stem and leaf style questions, wherein a question stem appears first (i.e., "Have you ever experienced the following on a phone or when online?") followed by leaves ((a) [X]? (b) [Y]? (c) [Z]?) places a high cognitive burden on respondents to retain the stem throughout question administration. Better quality data is achieved through integrating the stem into each leaf to create separate, stand-alone questions (i.e., (1) Have you ever experienced X on a phone or when online? (2) Have you ever experienced Y on a phone or when online? (3) Have you ever experienced Z on a phone or when online?)

Reduce cognitive burden when assessing recency by asking about timing of most recent use rather than use within a certain period

Asking respondents whether they have experienced something in a preset period of time ('In the last three months have you …?') places a high cognitive burden on the respondent. They must consider whether they have experienced the particular situation, they must calculate when the time period in question occurred, and they must consider whether their experience falls within that time period. We found that some respondents struggled to complete these three mental processes, and instead recalled what they experienced at the reference period time (i.e., three months ago) or recalled the experience but were unsure if it fell within the pre-set time period (i.e., 'I experienced this last week; I don't know about three months ago.') We propose assessing recency by asking the respondent whether they have 'ever [experienced X]' then asking 'When was the last time you [experienced X]?' The enumerator can then place the respondent's reply in an appropriate time category, discussed next.

Measure recency according to response categories that allow for analysis that accounts for wide range of potentially relevant time periods

When asking 'When was the last time you [experienced X]?', the enumerator should categorize the respondent's answer in an appropriate time category, according to response categories presented in Table 2 below. Recognizing that different incidents may occur at varying frequencies, we aim to establish an 'ever occurred' baseline and then assess recency without rigidly tying it to a specific time window, which may or may not align with the relevant context. Depending on the level of granularity required for your programmatic or analytic data needs, either of the two options may be appropriate for use. Throughout this toolkit we have presented the mutually exclusive time categories option (the first column in Table 2) because each response option is unambiguous and discrete. However, this response option requires enumerators to convert the types of natural language responses they will receive ('today,' 'yesterday', 'this week', etc.) into the specific predefined categories. Careful training of enumerators will be required to ensure that they can accurately categorize the responses provided.

Table 2. Recommended survey question for measuring recency

Question: When was the last time you [experienced X]?	
Response options: **Depending on the context, response options A or B should be selected. Response option B** may be more convenient to administer, especially in communities with low literacy.	
Mutually exclusive time categories	**Overlapping natural language time categories**
1. Less than 24 hours ago 2. 2 - 7 days ago 3. 8 - 14 days ago 4. 15 - 31 days ago 5. More than 1 month but less than 3 months ago 6. More than 3 months ago but within the last 1 year 7. More than 1 year ago	1. Today or yesterday 2. Within the last week 3. Within the last two weeks 4. Within the last month 5. Within the last three months 6. Within the last year 7. More than one year ago

Avoid double negatives

Avoid questions that ask about something negative because if the respondent has not done or disagrees with the negative in the question, identifying the appropriate response option is confusing.

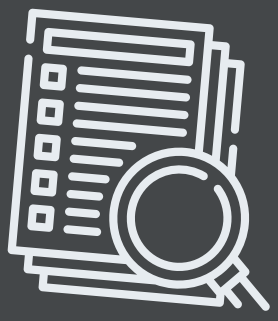
Use explainer boxes where relevant

Explainer boxes (Table 3) should proceed with terms which may be interpreted differently by individuals to ensure common, shared understanding. Internet boxes required to explain terms associated with harms are in the sections below. However, overarching terms may need to additionally be considered, including the internet, social media, WhatsApp, etc.

Table 3. Illustrative explainer boxes

Internet
Just for your information, someone would be using the Internet when they are doing any of the following: • Searching something on Google, YouTube etc. (add locally relevant examples) • Using Instagram, Facebook, TikTok, Twitter etc. (add locally relevant examples) • Sending messages or videos on WhatsApp, Telegram, Facebook Messenger, Gmail, etc. (add locally relevant examples) • Browsing or buying something on Amazon, Flipkart etc. (add locally relevant examples) • Sending money through Google Pay, Airtel Money etc. (add locally relevant examples) • We also want to tell you that Google, YouTube, Facebook, WhatsApp, etc. that we were just talking about are called 'apps'.
Personal information
Personal information means any details that can be used to identify you or find out more about you. This can include: • **Your name** (full name, nickname, or username) • **Contact details** like phone number, email address, or home address • **Date of birth** or age • **Photos or videos** of you or your family • **Government ID numbers** such as, national ID, passport, or driver's license • **Bank details** including account number, or PIN • **Login details** like passwords or PINs for your mobile device • **Location information** such as GPS or check-ins

3.0 Recommended survey questions



We use the measurement framework outlined above to guide the development of a quantitative measurement approach to assessing digital harms through population-based surveys in low-resource settings. In the following section, we focus on the prevalence of a core set of digital harms, their periodicity (recency and frequency), perpetrators of these harms, the response to the harm, and its impact.

3.1 Overarching questions on technology access

Access to technology is a major determinant of the experience of harms related to technology use [24]. The type and extent of these harms often vary depending on the nature of technology access. Key factors include the type of device ownership (e.g., individual vs. shared ownership), type of mobile phone owned (feature phone vs. smartphone), and internet accessibility [25]. In addition, the functionality of digital devices and the amount of time spent using them or being online can increase the likelihood of experiencing digital harms.

Table 4 below presents a set of high-level questions designed to measure participants' technology access before introducing the survey questions on harms. This step provides interviewers with important context and ensures a clearer understanding of each participant's level and nature of technology access. All questions in Table 4 were adapted from global surveys by the UCT Metrics team and cognitively tested in India, Kenya, and Nigeria.

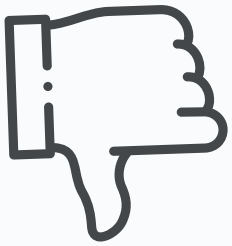
Table 4. Survey questions for measuring device access

Measurement element	Question	Response	Source
Mobile phone ownership	Do you own a mobile phone?	1.Yes 2.No	DHS-8, MICS-6 and After Access 2022; cognitively tested by UCT Metrics team in India, Kenya, and Nigeria (2023-24)
Access to shared mobile phone	[For respondents who report that they do not own a mobile phone] You said that you do not own a mobile phone, but is there a mobile phone that you use?	1.Yes 2.No	Adapted by UCT Metrics team from Gallup and GSMA Consumer Survey 2022; cognitively tested in India, Kenya, and Nigeria (2023-24)

Measurement element	Question	Response	Source
Computer	Do you own a computer or tablet?	1.Yes 2.No	Developed by UCT Metrics team
Phone type	What type of mobile phone do you have?	1. Smartphone 2. Feature phone 3. Basic phone	Developed by UCT Metrics team; cognitively tested in India, Kenya, and Nigeria (2023-24)
Phone condition	[If the phone is not observed, reported estimates can be solicited] Can the mobile phone remain on without being connected to the charger?	1. Yes 2. No	Developed by UCT Metrics team; Kilkari Impact Evaluation
	Is the screen cracked so severely that content cannot be read?	1. Yes, Screen Cracked 2. No, Screen Intact	
	Does the touch screen work and/or all keys work?	1. Yes, screen/ keys work 2. No, screen/ keys do not work	
Periodicity	When was the mobile phone within your reach yesterday? In the morning, in the afternoon, in the evening, or in the night?	1. Whole day 2. in the morning (6am - 12pm) 3. in the afternoon (12pm - 6 pm) 4. in the evening (6pm - 10pm) 5. in the night (10pm - 6 am) 6. Not at all	Developed by the UCT Metrics team; cognitively tested in India, Kenya, and Nigeria (2023-24)

Measurement element	Question	Response	Source
Internet use	Have you ever used the internet? (e.g. YouTube, WhatsApp, Google, Facebook, Instagram, etc.)	1.Yes 2. No	Adapted by UCT Metrics team from DHS-8, MICS-7, GSMA Consumer Survey 2022, and After Access 2022; cognitively tested in India, Kenya, and Nigeria (2023-24)
	When was the last time you used the internet?	1. Less than 24 hours ago 2. 2 - 7 days ago 3. 8 - 14 days ago 4. 15 - 31 days ago 5. More than 1 month but less than 3 months ago 6. More than 3 months ago, but within the last 1 year 7. More than 1 year ago	Developed by the UCT Metrics team; cognitively tested in India, Kenya, and Nigeria (2023-24)

3.2 Digital violence



Digital violence refers to harmful behaviors and actions carried out through digital technologies, online platforms, or electronic communication tools, with the intent to intimidate, control, harass, exploit, or cause harm [8]. We have classified digital violence into (1) online technology facilitated violence, including sexual harassment and abuse, and doxxing, as well as (2) off-line technology facilitated violence, including emotional, verbal or physical abuse that is triggered, escalated, or justified by the use of digital technologies.

3.2.1 On-line technology facilitated violence

Onl ine technology facilitated violence involves the use of digital technologies to intentionally humiliate, annoy, attack, threaten, alarm, or offend individuals [26].

While digital violence covers any purposely cruel and targeted communication online or over the phone, there are several specific sub-types, including: cyberstalking (persistent harassment, intimidation, or monitoring through electronic communication), cyberbullying (repeated hostile behavior targeting an individual, often youth), online hate speech and image-based abuse. These forms of digital violence can be sexual in nature, and/or target identities such as race, caste, class, gender, and religion.

In the section that follows, we provide a question to measure the prevalence of digital violence in general, and questions to measure sexual digital violence and doxxing. The prevalence question should be followed by the standard format of questions on recency, frequency, medium, perpetrator, impact, and response of digital violence as outlined in Annex 2.

In the section that follows, we provide a question to measure the prevalence of digital violence in general, and questions to measure sexual digital violence and doxxing.

Table 5. Survey question for measuring the prevalence of digital violence

Measurement element	Question	Response	Source
Prevalence of digital violence	Have you ever received any offensive and unwanted calls, messages, photos or videos on a mobile phone or on the internet? [Enumerator note: this includes anything from mobile phone calls and text messages to internet communication such as comments in Facebook/ Instagram, messages on chat apps like WhatsApp, and emails, etc.]	1. Yes 2. No	Adapted by UCT Metrics team from GSMA Consumer Survey 2023; cognitively tested in Kenya, and Nigeria (2023-24)

Key considerations:

- During cognitive testing, respondents noted having received 'upsetting' content including videos of car crashes or news events. To ensure that this content is not captured under this domain, the term "offensive" is being used in lieu of 'upsetting'.

Sexual digital violence

As noted above, digital violence can be sexual in nature, such as unwelcome sexual comments or requests, as well as image-based sexual abuse. Image-based abuse includes: (i) **revenge porn**: the online distribution of sexually graphic photographs or videos without the consent of the individual in the images [27], (ii) **upskirting**: taking a photo under a person's clothing without their permission [28], (iii) **sexting coercion**: coercing someone into sharing intimate images [29], (iv) **sextortion**: making threats to share nude or sexual images to coerce the victim into complying with certain demands, such as paying a ransom, sharing intimate images, or engaging in unwanted acts [30], (v) **deepfakes** (using artificial intelligence (AI) to create deceptive and non-consensual sexual explicit content) [31], and (vi) **cyberflashing** (sending unwanted images or videos of genitals) [32].

In the section to follow we provide survey questions to measure the prevalance of different forms of online sexual violenc (Table 6 below, which should then be followed with the standard format of questions on recency, frequency, medium, perpetrator, impact, and response of online sexual violence (Annex 3).

Table 6. Survey questions for measuring the prevalence of sexual digital violence

Measurement element	Question	Response	Source
Unwanted sexual comments	Has someone ever made unwanted sexual comments to you over the phone or on the internet? For example {YouTube, Instagram, Facebook, WhatsApp, Google-- insert locally relevant examples}	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested
Unwanted sexual requests	Has someone ever asked you to do something sexual that you did not want to do on phone call or on the internet? For example {YouTube, Instagram, Facebook, WhatsApp, Google-- insert locally relevant examples}	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested

Measurement element	Question	Response	Source
Image based abuse			
Revenge porn	Have private [insert local terms] photos or videos of you that are sexual in nature ever been sent to others on the phone or internet without your permission?	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested
Upskirting	Have private [insert local terms] photos or videos showing your body ever been taken without your permission?	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested
Sexting coercion	Has anyone ever threatened or forced you to send them private [insert local terms] photos or videos showing your body over the phone or internet?	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested
Sextortion	Has anyone ever threatened to share private [insert local term] photos or videos of your body with others over the phone or internet unless you gave them money?	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested
Deepfakes (non-sexual)	Has anyone ever created or changed a photo, video, or audio recording of you so that it looked or sounded real, but was not?	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested
Deepfakes of a sexual nature	Have you ever seen a video or photo where your face or voice has been changed, so it looks like you are saying or doing something sexual, but in reality, it is not true?	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested
Cyberflashing	Has anyone ever sent you private [insert local terms] photos or videos of themselves or someone else on social media or using a chat app like (WhatsApp, Telegram, Messenger, Signal, etc.), when you did not want it?	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested

Key considerations

- The question seeking to assess revenge porn may be hard to administer because it hinges on an assumption that the respondent has allowed photos or videos of sexual nature to be taken of them in order to ask whether these have been improperly used (i.e. as revenge). Among people who have never had such photos taken or videos made, even asking about this could be deemed insulting.
- Cognitive interviews indicated that framing these behaviors under a single umbrella term (e.g. Have you ever experienced image-based abuse, including revenge porn, sexual coercion, or unwanted images or videos of someone's intimate parts/genitals?) was not well understood by respondents. Therefore, each sub-type should be assessed through stand-alone questions to ensure accurate measurement of prevalence.
- The concept of "permission" may be understood differently across contexts, particular among low-literacy populations in rural India. Replacing this term with "without telling you", could improve comprehension; however, this phrasing would not fully capture the idea of consent. For example, a person might inform someone that they are sharing a photo yet still do so without that person's agreement.
- Cognitive interviews in India revealed that respondents often interpreted the English word "permission" as a matter of courtesy rather than social control. Because mobile phones are commonly shared within families, asking permission was usually seen as polite behavior, not a restriction. In this context, permission is best measured in relation to phone ownership – e.g. where a phone owner must ask someone else before using their own phone, or a person must always seek approval before using a shared phone.
- We do not provide questions regarding online sexual trafficking and exploitation as measurement has legal and ethical ramifications and is considered beyond the remit of this guide. Online sexual trafficking and exploitation refers to a criminal conduct in which digital technologies, internet platforms or other online sources are used to facilitate the recruitment, coercion, or exploitation of individuals, especially vulnerable groups, for sexual purposes [32, 33]. It often includes actions such as grooming, coercion, live streaming, sexual abuse and the production or distribution of child sexual abuse material online.

Doxing

Doxing refers to the act of exposing personal or private information about someone without their consent with intentions of causing harm [34]. Although doxing is a violation of privacy and data protection, it is usually categorized as a form of digital violence because of the intention to harm [35, 36]. In the section, questions to measure the prevalence of doxing are proposed, followed by the standard format of questions on recency, frequency, medium, perpetrator, impact, and response as described in Annex 4.

Table 7. Survey questions for measuring the prevalence of doxing

Measurement element	Question	Response	Source
Explainer box on personal and private information	Personal information means any details that can be used to identify you or find out more about you. This can include: **Your name** (full name, nickname, or username) **Contact details** like phone number, email address, or home address **Date of birth** or age **Photos or videos** of you or your family **Government ID numbers** such as, national ID, passport, or driver's license **Bank details** including account number, or PIN **Login details** like passwords or PINs for your mobile device **Location information** such as GPS or check-ins		
Prevalence of doxing	Has someone ever shared your personal information on the internet without your permission? [Enumerator note: You can clarify that this is also called doxing.]	1. Yes 2. No	Adapted by UCT Metrics team from GSMA Consumer Survey 2023; cognitively tested in India, Kenya, and Nigeria (2023-24)

3.2.2 Off-line technology facilitated violence

Emotional and verbal abuse

Emotional and verbal abuse encompasses a broad range of behaviors that harm another person's emotional well-being. These may include verbal (spoken or written) insults, threats, humiliation, yelling, isolation, intimidation, controlling behaviors, degradation, destruction of property, and even sexual coercion [37, 38]. Emotional abuse can be both verbal and nonverbal, and often involves repeated patterns designed to erode self-worth and autonomy [37, 38].

In the following section, we provide a set of survey questions to measure the prevalence of offline emotional or verbal abuse attributed to the use of digital devices. These can be followed by survey questions on the recency, frequency, perpetrator, impact and response, shown in Annex 5.

Table 8. Survey questions for measuring the prevalence of emotional and verbal abuse

Measurement element	Question	Response	Source
Verbal abuse in response to phone damage	[Read the explainer box] Has someone ever verbally hurt/scolded you for breaking or damaging a phone, tablet or computer?	1. Yes 2. No	Developed by the UCT Metrics team; cognitively tested in India, Kenya, and Nigeria (2023-24)
Verbal abuse in response to technology use	Has someone ever verbally hurt/ scolded you for spending too much time on the phone or internet? For example {YouTube, Instagram, Facebook, WhatsApp, Google-- insert locally relevant examples}	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested
	Has someone ever verbally hurt/ scolded you for using the internet? For example, {YouTube, Instagram, Facebook, WhatsApp, Google-- insert locally relevant examples}?	1. Yes 2. No	Developed by the UCT Metrics team; cognitively tested in India, Kenya, and Nigeria (2023-24)
	Has someone ever verbally hurt/scolded you talking to people your family does not know on a mobile phone, tablet or the internet? For example {YouTube, Instagram, Facebook, WhatsApp, Google-- insert locally relevant examples}	1. Yes 2. No	Developed by the UCT Metrics team; cognitively tested in India, Kenya, and Nigeria (2023-24)
	Has someone ever verbally hurt/scolded you for posting videos or photos of yourself on the internet? For example, on {YouTube, Instagram, Facebook, WhatsApp, Google-- insert locally relevant examples}.	1. Yes 2. No	Developed by the UCT Metrics team; cognitively tested in India, Kenya, and Nigeria (2023-24)

Physical violence

Offline physical violence triggered by digital technology refers to physical harm such as burning, kicking, beating, or punching, that is linked to the use of digital devices. In the following section, we provide a set survey questions to measure the prevalence of physical violence attributed to the use of digital devices and solutions. This is followed by survey questions on the recency, frequency, perpetrator, impact and response shown in (Annex 6).

Table 9. Survey questions for measuring the prevalence of physical violence

Measurement element	Question	Response	Source
Physical violence in response to phone damage	Has someone ever hit you or hurt you in for breaking or damaging a mobile phone, tablet or computer?	1. Yes 2. No	Developed by UCT Metrics team; cognitively tested in India, Kenya, and Nigeria (2023-24)
Physical violence in response to technology use	Has someone ever hit you or hurt you in for *spending too much time* on the phone or internet? For example {YouTube, Instagram, Facebook, WhatsApp, Google-- insert locally relevant examples}	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested
	Has someone ever hit you or hurt you in for using the phone or internet? For example {YouTube, Instagram, Facebook, WhatsApp, Google— insert locally relevant examples}?	1. Yes 2. No	Developed by UCT Metrics team; cognitively tested in India, Kenya, and Nigeria (2023-24)
	Has someone ever hit you or hurt you in for *talking to people your family does not know* on the phone or internet? For example {YouTube, Instagram, Facebook, WhatsApp, Google-- insert locally relevant examples}	1. Yes 2. No	Developed by UCT Metrics team; cognitively tested in India, Kenya, and Nigeria (2023-24)
	Has someone ever hit you or hurt you in for *sharing or posting videos or photos of yourself* on the internet? For example, on {YouTube, Instagram, Facebook, WhatsApp, Google-- insert locally relevant examples}	1. Yes 2. No	Developed by UCT Metrics team; cognitively tested in India, Kenya, and Nigeria (2023-24)

Key considerations:

- Qualitative interviews conducted in India, Kenya and Nigeria explored how violence linked to technology use is experienced and understood. Initially, questions were designed to capture any form of violence – whether verbal or physical – as a single category. However, findings indicate the need to distinguish between physical violence and verbal reprimands such as 'scolding,' which participants perceived as more frequent and less severe. Therefore, the current question set includes an explainer box that clearly defines physical violence, allowing its prevalence to be measured separately.
- Questions on physical violence can be broken down into specific use cases – for example, making phone calls to someone unknown to your spouse or family. These use cases should ideally be derived following qualitative research and be context specific.
- The Demographic and Health Surveys include a series of questions that assess attitudes towards physical violence. Annex 1 contains these questions along with response options that include a digital component.
- The separation of mental and physical health impacts may be necessary in some cases, as experiences of physical violence can lead to physical harm, psychological harm, or both. To capture this variation, we provide response options for both physical and psychological impacts following exposure to physical violence, ensuring that the measurement of impact is comprehensive and accurate.

3.3 Misinformation, disinformation and malinformation

The concepts of **misinformation, disinformation, and malinformation** all involve the sharing of false, misleading, or harmful information. They are distinguished primarily by the *intent* behind the act of sharing. Because intent is not always clear or easy to determine, and because the concepts often overlap, these phenomena are often better measured through **in-depth interviews** or **secondary analyses** of social media and related data.

In the section below, we focus on the measurement of false information and under key considerations provide added questions for measuring misinformation, and disinformation. When we attempted to fully separate these categories, the additional wording created confusion among respondents. To address this, we simplified the questions to make them easier to understand, particularly for respondents with lower literacy levels.

Misinformation is the sharing of false or inaccurate information without the intent to cause harm [15]. For example, during the pandemic, messages shared over WhatsApp included that drinking hot lemon water every morning can "kill" the COVID-19 virus in your throat before it reaches your lungs. While there is no scientific evidence to support this claim it can give people a false sense of protection, potentially leading them to ignore proven measures like vaccination, mask-wearing, or hand hygiene.

Comparatively **disinformation** is false information that is deliberately created and shared with the intention to deceive or cause harm to an individual, group, organization or country [15]. A pertinent example of this would be a WhatsApp message claiming that voting days or stations had been changed, in an effort to prevent people from exercising their right to vote. The information is false, intentional and can cause harm. Disinformation includes the creation and sharing of "deepfakes", which are manipulated or entirely synthetic media (images, video, audio) created using deep learning–based techniques [39].

Malinformation involves the sharing of *truthful information* with the intent to cause harm. This may involve taking information out of context, releasing it at a sensitive moment, or leaking private facts [15].

Throughout this toolkit, we focus on **survivors of harm** rather than the **perpetrators**. Accordingly, we emphasize the broader concept of *false information*. For surveys where identifying perpetrators is important, follow-up questions may be used to distinguish between misinformation (falsehood shared without harmful intent) and disinformation (falsehood shared with harmful intent). However, accurately separating these categories requires a reliable assessment of intent—something that is difficult to achieve through self-reported surveys.

Measuring **malinformation** poses an additional challenge. Because it involves truthful information used to harm, it generally requires presenting respondents with concrete examples to ensure understanding. These challenges are further discussed under Key Considerations below. In the following section, we provide a way to measure the prevalence of false information attributed to the use of digital devices and solutions. This is followed by survey questions on the recency, frequency, perpetrator, impact and response shown in (Annex 7).

Table 10. Survey questions for measuring false information

Measurement element	Question	Response	Source
False information	Have you ever heard or seen information on your phone that you thought was not true?	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested

Key considerations

- The phrase "seen information" has been used to enable the inclusion of individuals that are not able to read and therefore may have watched a video or listened to a voice note which was not true.
- For some users, phone use may be constrained to watching entertainment videos (e.g. music or cooking) that do not convey information that could be true or false (i.e. it's just song). For this sub-set of users, responses may be meaningless because they may answer "no" to the question of "Have you ever seen information on your phone that you thought was not true?". In such contexts either a "not applicable" option could be added to the response options or rather, it may preferrable to measure this concept through qualitative interviews where more nuanced discussions are possible.
- To measure **disinformation,** a follow up question to the one provided above could be considered to respondents that answer "Yes". This follow up question could say "[If yes] Did you share that information?". Respondents who answer in the affirmative could then be classified as having spread disinformation.
- To measure **misinformation**, the question *"Have you ever shared information on the phone or internet that you later found out was not true? For example, through SMS, WhatsApp, telegram, or by posting it on the internet?"* may be appropriate for further cognitive testing.
- To measure **malinformation,** we considered the potential survey question *"Has anyone ever shared true information about you over the phone or internet in a way that hurt you?"*. However, use of this question risks ambiguity. The question could be misinterpreted by the respondent to suggest that there is indeed true information out there that could hurt them. Further questions should be developed through qualitative research.

Verifying information

Many surveys endeavor to ask respondents about their reported ability to verify whether information seen or received online is true. The table below presents a series of questions designed to assess whether, and in what ways, individuals verify the truthfulness of information they have seen or read on the internet, or in phone messages. Questions have been worded carefully to avoid leading respondents and minimize social desirability biases in the responses. By anchoring the question to the most recent time the activity occurred, we have sought to minimise recall biases and improve response accuracy.

Table 11: Survey questions for measuring information verification

Measurement element	Questions	Response	Source
Verification	Have you ever checked if information you saw on your phone was true?	1. Yes 2. No	Adapted by UCT Metrics team from MICS-7; cognitively tested in India, Kenya, and Nigeria (2023-24)
Recency	[If yes to the above question] When was the last time you did this?	1. Less than 24 hours ago 2. 2 - 7 days ago 3. 8 - 14 days ago 4. 15 - 31 days ago 5. More than 1 month but less than 3 months ago 6. More than 3 months ago, but within the last 1 year 7. More than 1 year ago	Developed by the UCT Metrics team; cognitively tested in India, Kenya, and Nigeria (2023-24)
Medium	Thinking about the last time, how did you check to see if the information you saw or read on the internet or in phone messages (e.g. SMS, WhatsApp, Telegram, Signal, Messenger etc.) is true?	1. Checked multiple sources 2. Consulted fact-checking websites (e.g., Snopes, FactCheck.org) 3. Looked at author's credentials 4. Considered the reputation of the website 5. Asked someone knowledgeable 6. Other specify	Developed by UCT Metrics team; needs to be cognitively tested

Key considerations:

- Cognitive interviews found that respondents could give clearer answers when given a benchmark event. Thus, in addition to "have you ever" questions to establish prevalence, we recommend asking medium, response and other follow-on questions about a specific event "The last time…"
- The ITU's Digital Skills Indicator asks: "In the last three months, have you verified the reliability of information found online?" However, cognitive interviews showed that respondents struggled to understand the terms "verify" and "reliability". The phrase "information found online" was also considered too vague, and its intent was unclear. To address this, clearer alternatives include: A) Have you ever checked if information you found online was true? B) [If yes] When was the last time you did this??

3.4 Privacy and Data Protection

In digital environments, violations of privacy and data protection can take many forms. For the purposes of population-based quantitative research, we identify seven core categories of privacy and data-related harms that reflect the most common risks: (i) **identify theft**, (ii) **surveillance and tracking**, (iii) **data breaches**, (vi) **consent and autonomy violations**, (v) **data misuse**, (vi) **data profiling and discrimination**, and (vii) **rights to erasure violations**. This categorization, which builds on frameworks such as that developed by the Information Commissioner's Office in the UK [40] aims to support both conceptual clarity and the development of robust survey instruments. In the sections that follow, we outline how to measure prevalence across these key domains. Each prevalence question can be paired with a standard set of follow-up items on recency, frequency, medium, impact, and response, as detailed in **Annex 8**.

During cognitive interviews in India, concepts such as privacy policy, personal data, and hacking were found to be largely unfamiliar to respondents, often leading to confusion and misinterpretation. Explaining these terms in ways that resonated with local language and everyday experiences proved challenging. In such contexts, qualitative research may be a more promising avenue for gathering evidence on respondent perceptions and practices.

3.4.1 Identify theft

Identify theft refers to the unauthorized acquisition or use of personal information—typically online—with the intent to commit fraud or related crimes [41]. In the context of digital harms, identity theft extends beyond financial fraud. It can include the misuse of personal data to impersonate individuals online, gain access to private accounts, spread misinformation, damage reputations, or harass victims.

Table 12. Survey questions for measuring identity theft

Measurement element	Questions	Response	Source
Identity theft	Has anyone ever used your personal details, like your ID or bank details, without asking you, to pretend to be you or do something wrong?	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested

Key considerations:

- Cognitive testing in India found that the term "personal information" could mean family secrets or personal preferences. To enhance comprehension, "personal details" (such as "your bank details", "your personal ID"), was adopted as a more accessible alternative.
- The questions have been designed to be self-explanatory, so that explainer boxes are usually not required. Explainer boxes should only be used when essential because respondents do not retain a lot of information.

- If cognitive testing indicates that an explainer box is required for the question above, we suggest the following:
    - *[Explainer box] Identity theft happens when another person uses your personal details—like your name, ID number, or bank information—without your permission, in order to trick, cheat, or do something wrong*

3.4.2 Surveillance and tracking

Surveillance refers to the use of personal data to monitor, control, or regulate individual behavior. **Dataveillance** is a related concept, describing the automated and systematic monitoring of people's actions or communications through digital data systems [42]. **Tracking** refers to the collection and use of data about an individual's behavior across different contexts, often extending beyond the original purpose for which the data was given [42]. Because surveillance and tracking often occur passively—without the user's awareness—they are difficult concepts to measure through surveys, particularly in low-literacy or low-digital-exposure populations. These terms involve a level abstraction that may exceed the everyday experience or familiarity of many participants..

During qualitative interviews, the concept of *surveillance* was examined through the lens of *supervision*, which conveys active monitoring rather than passive observation. Findings from cognitive interviews in India revealed a conceptual blurring in how respondents understood this form of social control. When asked whether they were supervised while using a phone—for calling, messaging, or watching videos—participants struggled to provide clear explanations. This difficulty was partly due to the fact that many respondents shared their phones with family members. In such cases, relatives might casually look through call logs or browsing history, which participants perceived as passive checking rather than deliberate monitoring.

These insights suggest that active supervision or surveillance is most clearly understood in contexts where individuals own their own phones, as shared ownership complicates perceptions of control. In the section to follow, questions to support the measurement of surveillance and tracking are proposed with alternatives provided for phone owners and phone sharers.

Table 13. Survey questions for measuring surveillance and tracking

Measurement element	Questions	Response	Source
Call records/ history	[For phone owners] Does somebody in your family / your partner check who you have called or received calls from on your phone? [For non-owners] Does somebody in your family / your partner check who you have called or received calls from on the phone you use? [Enumerator note: this includes checking any calls including on apps WhatsApp, etc.]	1. Yes 2. No	Developed by the UCT Metrics team; cognitively tested in India, Kenya, and Nigeria (2023-24)

Measurement element	Questions	Response	Source
Messages	[For phone owners] Does somebody in your family / your partner check the messages you send or receive on your phone? [For non-owners] Does somebody in your family / your partner check the messages you send or receive on the phone you use? [Enumerator note: this includes checking any text messages, including SMS messages, and messages on chat apps like WhatsApp, etc.]	1. Yes 2. No	Developed by the UCT Metrics team; cognitively tested in India, Kenya, and Nigeria (2023-24)
Browsing history	Does somebody in your family / your partner check what you search on Go ogle or watch on places like YouTube?	1. Yes 2. No , no one checks 3. No, I don't use google or social media	Modified, needs cognitive testing
Contacts	Does somebody in your family / your partner check which friends or contacts you have on {insert relevant local examples of social media such as Facebook/ WhatsApp / Instagram / Snapchat / TikTok}?	1. Yes 2. No	Developed by the UCT Metrics team; cognitively tested in India, Kenya, and Nigeria (2023-24)

Key considerations:

- Questions on the concept of "watching" was explored through cognitive interviews [18]. Communicating the concept of surveillance required careful attention to language in India. The Hindi term *nigrani* (supervision) was not widely understood, whereas *nazar rakhna* (keeping an eye on) communicated the intended meaning more effectively than *dekh rekh* (watching over).
- In lieu of binary Yes/ No response options, a 3-point Likert scale can be used (1-Never, 2-Rarely, 3-Often). Using this response requires a minor adjustment to the parent question's wording to incorporate the clause: "Would you say this happens….". For example, "Does somebody in your family / your partner check your browsing history or what you search on Google or YouTube? Would you say this happens…. 1-Never, 2-Rarely, 3-Often."

3.4.3 Data breaches

A **data breach** is the accidental or deliberate loss, theft, alteration, or unauthorized access to personal data [41]. Such breaches can occur through human error, system flaw or hacking. **Hacking** refers to the act of manipulating or gaining unauthorized access to a computer system, network, or digital device to disrupt functions or gather sensitive information [43]. To communicate the concept of data breeches to low literate, mobile first populations, we have used the term 'hacking', which is better understood. Nonetheless, cognitive interviewing revealed significant variation in how the term "*hacking*" is understood across countries:

- **Nigeria and Kenya**: Respondents commonly associated hacking with someone gaining unauthorized access to their social media accounts, particularly Facebook. This reflects a localized understanding rooted in personal experience with compromised accounts.
- **India**: The concept was more often misunderstood. Respondents frequently interpreted "hacking" as the word "hanging," which refers to technical malfunction--such as a phone freezing, slowing down, or failing to work properly. Attempts to explain hacking failed to resonate. Only a small number of male respondents knew the term, reporting personal experiences of Facebook accounts being hacked.

These findings highlight the challenges of measuring digital harms across diverse settings. Although the term *"hacking"* is better understood than 'data breech', researchers must carefully adapt wording to local contexts to avoid misinterpretation and ensure accurate data collection. In the phrasing below, the addition of the second clause *"… have personal details been stolen from your phone"* serves as an explanation of what the term hacking is intended to mean. This added clause was found to reduce cognitive gaps between enumerators and respondents in India, Kenya and Nigeria and thus is recommended.

Table 14. Survey question for measuring the prevalence of data breaches

Measurement element	Question	Response	Source
Data breach	Has your phone ever been hacked, or have personal details been stolen from your phone?	1. Yes 2. No	Adapted UCT Metrics team from GSMA Consumer Survey 2023; cognitively tested in India, Kenya and Nigeria (2023-24)

3.4.4 Consent and autonomy violations

Within digital environments, consent violations occur when agreement to the collection or use of personal data is not freely given, informed, specific, or clear. These harms often arise through coercion, deception, or manipulative digital design practices. Common examples include confusing or hidden privacy settings that make it difficult to opt out of data sharing or forced opt-ins, such as being required to accept all cookies before accessing a website.

Autonomy violations are a distinct form of digital harm recognized within data protection frameworks, including the ICO's taxonomy of h arms [40]. They occur when individuals' ability to make informed and voluntary choices online is undermined—often through manipulative interface design, opaque data practices, or severely limited alternatives. These harms may result from excessive data collection, coercive consent flows, or profiling that nudges behavior without meaningful control. For instance, mobile applications that demand unnecessary permissions—such as access to photos, contacts, or login details— can erode user agency and compromise users' independence.

Together, consent and autonomy violations erode digital agency by reducing individuals' capacity to exercise genuine choice over how their personal data are collected, shared, and used [44]. Elsewhere we have explored beneficiary perceptions of consent for onward health data use in South Africa using qualitative research methods [45, 46]. Measurement of consent and digital autonomy violations through quantitative surveys is challenging in many low-literate, mobile first contexts where beneficiaries are unfamiliar with these concepts. Cognitive interviews conducted in India, Kenya and Nigeria sought to address these challenges but ultimately, findings showcased low resonance of these concepts. We therefore propose excluding these harms from population-based surveys and addressing them through qualitative methods instead.

3.4.5 Data misuse

Data misuse refers to the inappropriate or unauthorized use of personal data beyond its originally intended purpose. This can include activities such as sharing information with third parties without consent, exploiting data for personal gain, committing fraud, or engaging in practices that violate regulatory requirements or established best practices [47].

The concept of data misuse may be complicated to convey to respondents in some contexts. In the question below, we have sought to ensure respondents understand "personal information" by using the term 'personal details' and providing examples i.e. name and phone number. This is followed by examples of misuse. In many contexts, respondents may be unfamiliar or unaware that their information can be misused and therefore discussions around this may be better had through qualitative interviews. The question below provides a starting point for further refinement through cognitive testing depending on the research requirements.

Table 15. Survey question for measuring the prevalence of data misuse

Measurement element	Question	Response	Source
Data misuse	Has anyone ever used your personal details—like your name, phone number, or photo—in a way that you did not agree to? For example, sold your personal details to others who used the information to send you ads.	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested

Key considerations:

- If cognitive testing indicates that an explainer box is required for the question above, we suggest the following:
    - *[Explainer box]: Data misuse happens when your personal details-such as your name, phone number, email address, home address, or photos-are collected, shared, or used in ways you never agreed to. This could happen if:*
    - *A company sells your phone number to advertisers who then flood you with spam calls.*
    - *Your photo is used in an online ad without your permission.*
    - *A website shares your email address with someone else who then sends you marketing emails you never signed up for.*
    - *A website **tracks your online activity** and uses it to target you with ads, even though you.*

3.4.6 Data profiling and discrimination

Data profiling refers to the automated processing of personal data to evaluate, predict, or categorize individuals—often based on patterns or inferred attributes [48]. Discrimination occurs when such profiling leads to unfair or unequal treatment, especially of marginalized or vulnerable groups, whether intentionally or through biased algorithms or datasets [49]. These practices often operate invisibly and in abstract ways, making the resulting discrimination subtle, indirect, and difficult for individuals to detect or name. Because discrimination is also a socially sensitive topic, participants may hesitate to answer questions honestly, out of concern about stigma or reprisal. As a result, quantitative survey responses alone may not fully capture the scope or nuance of these experiences. To address this, quantitative data collection should be complemented with qualitative approaches that can provide deeper insights into how profiling and discrimination are perceived and experienced.

Table 16. Survey questions for measuring the prevalence of data profiling and discrimination

Measurement element	Question	Response	Source
Personalized ads / Targeting	Have you ever noticed ads or messages on your phone or the internet that seemed to know too much about you (for example, ads showed things you searched for on Google, Instagram, or YouTube)?	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested
Treated unfairly	Has anyone ever treated you unfairly because of things you did on your phone or on the internet—like the apps you used, messages you sent, or websites you visited?	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested
Lack of choice	Have you ever felt you had no real choice but to give personal details (like your ID, photo, or phone number) in order to use an app or website, even though you did not want to?	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested

Key considerations:

- If cognitive testing indicates that an explainer box is required for the question above, we suggest the following:
    - *[Explainer box]: Sometimes apps, websites, or computers collect information about what you do online—like what you search for, what you buy, or what you like to watch or read. They use this information to guess things about you, such as your interests, your habits, or even your money situation.*

3.4.7 Violations of the 'Rights to Erasure'

Erasure violations arise when individuals are unable to permanently delete personal data, resulting in the continued availability of outdated, sensitive, or other unwanted information. Such violations can carry reputational, social, and economic consequences, as articulated in the European Union's General Data Protection Regulation [50]. A frequently cited example is when individuals upload personal content—such as videos, photographs, or identifying details—that they later wish to withdraw but are unable to remove from digital platforms.

In many contexts, people may not fully understand what it means to delete something online. They might think that hiding, removing, or forgetting something on their phone or app all mean the same thing, which makes it difficult to answer questions about these experiences. This confusion is made worse by how online platforms work: even when someone tries to delete something, it is not always clear whether the information is truly gone, just hidden, or still saved somewhere behind the scenes. For researchers, this creates a challenge, because what people think has happened may not match what actually happens with their data, making it harder to measure erasure violations accurately.

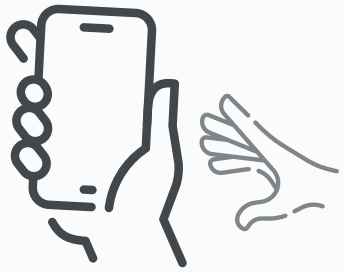
Table 17. Survey questions for measuring the prevalence of erasure violations

Measurement element	Question	Response	Source
Erasure violations	Have you ever tried to remove something about yourself (like your ID, photo, phone number, or a post) from an app or website, but couldn't do it?	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested

Key considerations:

- If cognitive testing indicates that an explainer box is required for the question above, we suggest the following:
    - *[Explainer box]: This happens when you cannot delete your details (like your name, photos, or posts) from websites or apps. Because of this, old or harmful information about you stays online.*

3.5 Digital fraud



Fraud is defined as any act that uses deception to achieve a gain [51]. **Digital fraud** is fraudulent activity that is enabled or facilitated by digital technologies such as the internet, mobile phones, or computers, where deception is used to obtain financial or personal gain [52]. Common forms of digital fraud include phishing, identity theft, social engineering attacks, online payment fraud, and cryptocurrency-related scams [53].

For the purposes of this toolkit, we focus on measuring the prevalence of **digitally enabled financial fraud**, which are traditional crimes that use digital tools to reach more victims, operate faster, or evade detection but are not inherently digital. Common examples include online shopping scams, romance scams, mobile money fraud, identity theft via phishing, and business email compromise for financial gain. Digitally enabled financial crime is currently the dominant form of digital fraud in terms of economic impact [54] and can be assessed through surveys with the general population.

Digitally dependent fraud, which uses methods like ransomware attacks and malware deployment, is challenging to measure through population-based surveys. These are better investigated using a combination of system log analysis and key informant interviews with specialists who can provide technical details and contextual information about the incident. Such groups may include IT staff or administrative personnel working within particular organisations or institutions.

In the sections that follow, we outline how to measure prevalence and types of digital fraud (Table 18 below). This can be be paired with a standard set of follow-up items on recency, frequency, medium, impact, and response, as detailed in **Annex 9.**

Table 18. Survey questions for measuring prevalence and types digital fraud

Measurement element	Question	Response	Source
Prevalence	Has your money ever been stolen over the phone or internet?	1. Yes 2. No	Adapted by UCT Metrics team from After Access; cognitively tested in India, Kenya and Nigeria (2023-24)

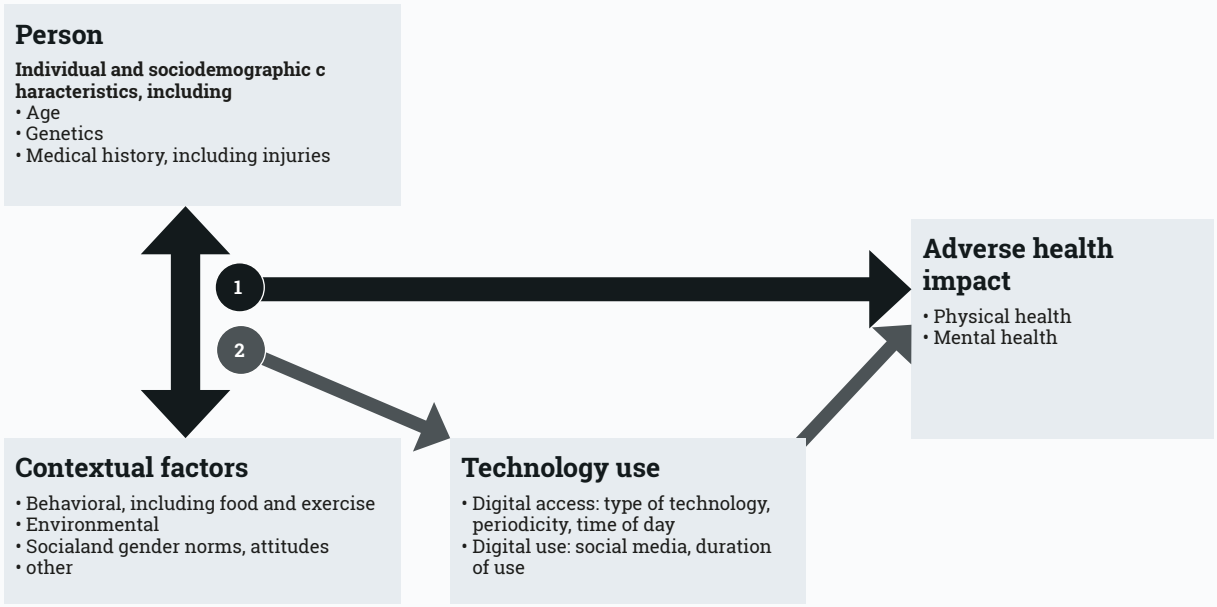
Measurement element	Question	Response	Source
Type of digital fraud experienced	[if yes to the above] What kind of scam was it? [Enumerator note: Select all that apply]	**1. Fake prize or lottery** Someone told me I won money or a gift, but I had to pay first and I never got anything. **2. Fake job offer** Someone promised me a job and asked for money or personal details, but the job was not real. **3. Mobile money scam** Someone tricked me into sending money through my phone (like M-Pesa, Airtel Money, etc.). **4. Message from a fake person** I got a message or call from someone pretending to be a friend, family member, or official, asking for money or help. **5. Online shopping scam** I paid for something online (like clothes or a phone), but I never received it. **6. Romance or friendship scam** Someone I met online said they loved me or wanted to help me, but they asked for money and then disappeared. **7. Bank or card fraud** Money was taken from my bank account or mobile wallet without my permission. **8. Asked to share private details** Someone tricked me into giving my ID number, password, or PIN — and then used it to steal money from me. **10. Other** Something else happened that felt like a trick or scam. (Please specify)	Developed by UCT Metrics team; needs to be cognitively tested

3.6 Health implications

Understanding the health implications of technology use is complex. Both physical and mental health outcomes are influenced by a range of individual and contextual factors, making it difficult to identify direct causal relationships. Most surveys, for example, are unable to capture the full range of mediating influences necessary to disentangle these effects.

Figure 3 shows how different factors interact to influence health risks. The black arrow links personal characteristics (like age, income, or education) with broader influences such as behavior, environment, and social and gender norms. These combined factors shape the likelihood of poor health outcomes. Technology, shown as a purple arrow, adds complexity. Technology can affect the link between personal/contextual factors and health in different ways: 1) It can hide the real cause, making it look like something else is responsible when it is not, for example increased screen time may seem to cause poor sleep while the real underlying issue anxiety from social media interaction. 2) It can change the strength or direction of the link, making a risk more dangerous, less harmful, or even flipping the effect, for example, prolonged used of mobile phone can exacerbate sedentary life hence posing a risk to physical health. 3) It can be part of the link itself, helping explain how one factor leads to another for example, high literacy level is linked to increased access and use of digital tools which further can lead to negative physical and mental health impacts .

Figure 3. Attributing technology use to adverse health outcomes



In addition to the challenge of untangling the impact of technology use on health outcomes, there is another issue: low-literate; mobile-first populations may not be familiar with the concepts researchers commonly use in health and tech studies. This can affect both the accuracy and reliability of measurements, particularly when abstract health concepts; like stress, mental well-being or risk perceptions, are interpreted differently across literary levels.

Based on these considerations, we propose a streamlined measurement approach that targets specific health conditions. Measuring these reliably may also be unrealistic, unless the survey is designed to focus specifically on the link between that health condition and technology use. In such cases, additional survey modules are needed, drawing on standardized tools (e.g. for measuring anxiety or depression), and expanding them with technology-related questions. These questions will require further cognitive testing and iterative refinement, especially as technology use evolves and public understanding grows.

3.6.1 Physical health implications

The physical health effects of digital technology use are gaining increasing attention, with growing evidence linking screen time and device use to a range of physical complaints [55]. The most commonly reported impacts include sleep disturbances [56], visual symptoms [57], musculoskeletal pain [58] and headaches [59].

Sleep disturbances

Using digital devices — especially social media — is associated with sleep problems. It might cause people to sleep less, sleep poorly, or take longer to fall asleep because their minds stay active. Sleep loss usually means getting less than 7 to 9 hours of sleep a night [47]. Measuring sleep disturbance is unlikely to be a priority for most programs and may be challenging to measure accurately, especially where self-reported sleep quality data is limited or subjective measures are difficult to validate. The section below provides a starting point for further cognitive testing.

To measure sleep quality the Pittsburgh Sleep Quality Index (PSQI) has been proposed, although cognitive testing of the survey questions is advised to further enhance phrasing and translation [60]. To explore how device use affects sleep, we propose survey questions that ask about phone use before and during sleep hours. We also include questions on where the phone is kept at night and whether it is on silent. These behaviours are treated separately, depending on whether they happen before sleep or during sleep disruptions. An adapted PSQI scale is included in **Annex 10**.

Table 19. Survey questions for measuring sleep disturbances and technology use

Measurement element	Question	Response	Source
Cumulative time on the device	In the last 24 hours, how much time have you spent on a mobile phone, tablet or computer? [Enumerator note: Responses can be observed or reported. If observed based on a smartphone app, clarify with the respondent, what amount of time in minutes they spent on the phone versus others noting that devices may be shared. If reported, estimate time in minutes; if hours are provided convert to minutes.	A. Reported time in minutes: B. Observed time in minutes:	Developed by UCT Metrics team; needs to be cognitively tested
	On a typical day, how much time do you usually spend on your phone, tablet or computer?	Reported time in minutes:	Developed by UCT Metrics team; needs to be cognitively tested
Device use prior to sleeping	What device do you usually use in the hour before sleeping?	1. Mobile phone 2. Computer 3. Tablet 4. None	Developed by UCT Metrics team; needs to be cognitively tested
Time spent yesterday on device prior to sleep	In the hour before trying to sleep yesterday, how much time did spend on the [insert device mentioned]?	Time in minutes [ ]	Developed by UCT Metrics team; needs to be cognitively tested

Measurement element	Question	Response	Source
Activities performed on the device	What activities were you doing on the device? [Enumerator note: Select all that apply]	1. Reading a book on the phone 2. Watching videos 3. Scrolling social media 4. Playing video or online games 5. Reading the news 6. Checking emails 98. Other [specify]	Developed by UCT Metrics team; needs to be cognitively tested
	Of the activities mentioned, what did you spend the most time on?	1. Reading a book on the phone 2. Watching videos 3. Scrolling social media 4. Playing video or online games 5. Reading the news 6. Checking emails 98. Other specify]	Developed by UCT Metrics team; needs to be cognitively tested
Average time spent on device prior to sleep	In the hour before trying to sleep, how much time do you usually spend on the [insert device mentioned]?	[ ] time in minutes	Developed by UCT Metrics team; needs to be cognitively tested
Device location during sleep	When you are sleeping, where is your device physically located?	1. Within reach 2. In the same room as me but not within reach 3. Outside the room	Developed by UCT Metrics team; needs to be cognitively tested
Device settings during sleep	Before going to sleep, is your device usually on 'sleep mode', the ringer and/or notifications on silent?	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested
Digitally impacted sleep	Do you usually fall asleep and stay asleep?	1. Yes 2. No	(Buysse et al., 1989)
Practices during disrupted sleep	When you have trouble falling asleep or wake up in the night, do you use your phone/tablet/computer?	1. Often 2. Rarely 3. Never	New question, needs cognitive testing.
	Thinking of the last time you had trouble falling asleep or woke up in the night, did you use your phone/tablet/computer?	1. Yes 2. No	New question, needs cognitive testing.

Visual disturbances

Due to the increase in digital access and use, "digital eye strain" also known as "computer vision syndrome" or "visual fatigue" have developed [61]. These encompass a range of symptoms that are broadly classified as; visual, ocular and extraocular [61] Predominant symptoms include: blurred vision while using technology, blurred vision when looking in the distance, difficulty refocusing eyes between distances, irritated or burning eyes, dry eyes, eye strain, tired eyes, sensitivity to light or eye discomfort [61]. A brief question on some common symptoms is included below. Depending on the scope of the research, this could be modified to encompass all the documented symptoms of computer vision syndrome in separate, simply phrased questions. These would again be best paired with the questions above quantifying digital use to establish a correlation between the two.

Table 20. Survey questions for measuring visual disturbances related to technology use

Measurement element	Question	Response	Source
Prevalence	Have you ever experienced eye pain, dryness, or discomfort when using or immediately after using your phone, tablet or computer?	1. Yes 2. No	Adapted from Seguí Mdel M. et al. (2015). *Journal of Clinical Epidemiology*, 68(6), 662–673; needs to be cognitively tested
Recency	[if yes] When was the last time you experienced these symptoms	1. Less than 24 hours ago 2. 2 - 7 days ago 3. 8 - 14 days ago 4. 15 - 31 days ago 5. More than 1 month but less than 3 months ago 6. More than 3 months ago but within the last 1 year 7. More than 1 year ago	
Frequency	[if yes] How often do you experience these symptoms?	1. Never 2. Rarely 3. Often	

Key considerations

- Isolating the impact of technology use on vision is challenging because a range of factors including age, may be associated with declining vision.
- Current questions have focused very generally on visual disturbances which may include a range of symptoms: burning sensation, eyestrain or dry eyes, light sensitivity, tearing, excessive blinking, redness, heavy lids, difficulty focusing, general visual discomfort when using a screen. Individual questions may be crafted to ascertain the prevalence of specific symptoms depending on research priorities.

Musculoskeletal complaints

Many musculoskeletal problems are linked to the way people sit, stand, or hold their bodies when using devices or working. Poor positioning can harm physical health — leading to bad posture, neck pain, back pain, and other related issues. In practice, muscle and joint problems may be more common in people who use computers for long stretches without moving, especially when sitting behind a desk. People who mainly use mobile phones can also develop symptoms. The most common is neck and shoulder pain, often called "tech neck." This happens when someone spends long periods looking down at a phone, computer, or other device putting repeated strain on the spine, muscles, and ligaments [58].

Table 21. Survey questions for measuring musculoskeletal complaints and technology use

Measurement element	Question	Response	
Data usage - duration	How much time do you typically spend using a phone, tablet, or computer each day and/or night?	[ ] time in minutes	New question, needs to be cognitively tested.
Prolonged Neck flexion	While using your phone, computer, or tablet, how often do you tilt your head downward for a long period of time?	1. Never 2. Rarely 3. Often	New question, needs to be cognitively tested.
Prevalence	Have you had pain, or stiffnessin your neck after using a phone, computer or tablet?	1. Yes 2. No	New question, needs to be cognitively tested.
Area of pain	[if yes, to question above] Where do you usually feel pain or stiffness after using your phone, tablet or computer? [Select all that apply]	1. Neck 2. Upper back 3. Shoulders 4. Between your shoulder blades O5. ther specify	New question, needs to be cognitively tested.
Improvement	Does your neck pain get better when you stop using a phone, computer or tablet?	1. Yes completely 2. Partially 3. No improvement	New question, needs to be cognitively tested.
Frequency	How often do you experience neck pain or stiffness?	1. Never 2. Rarely 3. Often	New question, needs to be cognitively tested.

Measurement element	Question	Response	
Recency	When was the last time you experienced neck pain or stiffness symptoms?	1. Less than 24 hours ago 2. 2 - 7 days ago 3. 8 - 14 days ago 4. 15 - 31 days ago 5. More than 1 month but less than 3 months ago 6. More than 3 months ago but within the last 1 year 7. More than 1 year ago	New question, needs to be cognitively tested.

Headache

Headaches may stem from a range of behavioral practices, including technology use [60]. In the following section, we propose a range of quantitative survey questions which can be used to establish a link between technology use and headaches.

Table 22. Survey questions for measuring headache resulting from technology use

Measurement element	Question	Response	Source
Data usage - duration	How much time do you typically spend using your phone, tablet or computer each day and/or night? [Enumerator note: if hours are provided, convert these into minutes. In many contexts, women's phone access is <1 hour per day hence minutes are the unit proposed.]	[ ] time in minutes	Developed by UCT Metrics team; needs to be cognitively tested
Prevalence	Have you ever experienced a headache during or immediately after using a phone, table, or computer?	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested

Measurement element	Question	Response	Source
Recency	When was the last time this happened?	1. Less than 24 hours ago 2. 2 - 7 days ago 3. 8 - 14 days ago 4. 15 - 31 days ago 5. More than 1 month but less than 3 months ago 6. More than 3 months ago but within the last 1 year 7. More than 1 year ago	Developed by UCT Metrics team
Frequency	How often do you experience headaches during or immediately after using a phone, table, or computer?	1. Never 2. Rarely 3. Often	Developed by UCT Metrics team; needs to be cognitively tested

Key considerations

- Casual association between technology use and headaches is challenging to establish because of the range of other factors which may cause headaches.
- Establishing the severity of the headache may be relevant but is difficult to measure and highly subjective.

3.6.2 Mental health implications

Digital technology use can have a significant impact on mental health. Researchers must consider a range of psychological outcomes, especially those linked to heavy or problematic social media use. This section outlines five mental health constructs relevant to digital harms, explains what they mean, describes common symptoms, and points to current evidence. It starts with an overarching question designed to establish the overall effect that technology has on a person's mental health.

Table 23. Survey questions for measuring the mental health implications of technology use

Question	Response	Source
Overall, has using a mobile phone had a positive or negative impact on your life? [Enumerator note: Do not read response options]	1. Negative impact 2. Neither negative nor positive impact 3. Both negative and positive impact 4. Positive impact 5. Don't know	Adapted by UCT Metrics team from GSMA Consumer Survey 2022; cognitively tested in India, Kenya and Nigeria (2023-24)

Anxiety

Anxiety is how the body and mind react to a perceived threat. It can show up as excessive worry, restlessness, irritability, fatigue, concentration problems, muscle tension, and disturbed sleep. It includes conditions such as generalized anxiety, social anxiety, and anxiety linked to relationships [56]. Anxiety symptoms have been increasingly linked to technology use, with studies showing associations between higher levels of social media engagement, digital multitasking, and elevated anxiety [63].

A widely used tool for measuring anxiety is the Generalized Anxiety Disorder 7-item scale (GAD-7), developed in 2006 by Spitzer, Kroenke, Williams, and colleagues as part of the PHQ family. The GAD-7 asks respondents how often they experienced symptoms such as persistent nervousness, uncontrollable worrying, difficulty relaxing, and feeling that something awful may happen during the last two weeks.

Responses are scored on a four-point scale (0 = not at all, 3 = nearly every day), yielding a total score from 0 to 21. Scores of 0–4 indicate minimal anxiety, 5–9 mild, 10–14 moderate, and 15–21 severe anxiety. While cognitive interviews in India, Nigeria, and Kenya found that frequency-based questions were more easily understood than agreement-based Likert scales, the GAD-7 remains a practical tool for categorizing anxiety severity. The questions are included as **Annex 11**, with table 24 recommending additional items for linking technology use and anxiety.

Table 24. Survey questions for establishing a link between technology and anxiety

Measurement element	Question	Response	Source
Prevalence	Have you ever felt anxiety symptoms, for example worried, restless, or unable to sleep because of using social media or other technology?	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested
Recency	[if yes] When was the last time I experienced these symptoms?	1. Less than 24 hours ago 2. 2 - 7 days ago 3. 8 - 14 days ago 4. 15 - 31 days ago 5. More than 1 month but less than 3 months ago 6. More than 3 months ago but within the last 1 year 7. More than 1 year ago	
Frequency	How often do you experience anxiety before/ after using your phone or computer?	1. Never 2. Rarely 3. Often	
Impact	How much do these anxiety symptoms affect your daily life (work/ study/relationships)?	1. Not at all 2. A little 3. A lot	

Social Media Addiction or Problematic Social Media use

Problematic Social Media Use (PSMU), often called Social Media Addiction (SMA), is understood as a type of behavioral addiction, similar to gambling or substance use disorders. It involves being overly focused on social media, using it to change your mood, needing more time on it to get the same effect, feeling uneasy when you cannot use it, having conflicts because of it, and returning to old habits after trying to stop [62]. Meta-analyses [63] highlight how these symptoms manifest in technology use, including excessive attention, uncontrollable urges to log on, devoting significant time and energy to social media, and interference with learning, responsibilities, relationships, and mental health.

To assess PSMU, the Bergen Social Media Addiction Scale (BSMAS) was developed and widely validated across cultural contexts. It measures **six core symptoms** each directly based on the *components model of addiction* (salience, mood modification, tolerance, withdrawal, conflict, and relapse). Responses to questions are provided using a Likert scale of agreement, which in this context was adapted from five to three points (never, rarely, often) for use among low-literacy populations. The BSMAS is a screening tool rather than a diagnostic instrument. There is no single score that defines problematic use, but higher scores suggest more severe issues. The tool is included as **Annex 12** and could be adapted through further cognitive testing for use in low resource contexts.

Depression and depressive symptoms

Depression is a common condition that can impair daily functioning, typically involving symptoms such as persistent low mood, loss of pleasure, changes in sleep or appetite, low energy, hopelessness, poor concentration, social withdrawal, and self-neglect [56]. Research increasingly shows links between social media use and depression. A meta-analysis covering over 450,000 individuals across 62 studies found a moderate association between problematic social media use and elevated depressive symptoms [64].

To assess depressive symptoms, the Patient Health Questionnaire (PHQ-9) is a widely used and validated tool [65]. This 9-item questionnaire asks respondents to rate the frequency of symptoms over the past two weeks on a four-point scale, generating scores from 0 (no symptoms) to 27 (severe depression). Scores of 10 or more typically indicate clinically significant depression, and researchers are ethically required to ensure support mechanisms for such respondents. The PHQ-9 is attached as **Annex 13**, with additional recommended items for linking technology use and depression provided in table 25.

Table 25. Survey questions for establishing a link between technology and depression

Measurement element	Question	Response	Source
Perceived link with technology use (Aggravation)	Do you feel that your use of the phone or computer has an impact on your mental health?	1. No impact 2. Positive impact (improves mental health) 3. Negative impact (worsens mental health)	Developed by UCT Metrics team; needs to be cognitively tested

Measurement element	Question	Response	Source
Prevalence	[With reference to the PHQ9] Have you ever felt these symptoms after you use your phone or computer?	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested
Recency	[If yes] When was the last time you experienced these symptoms?	1. Less than 24 hours ago 2. 2 - 7 days ago 3. 8 - 14 days ago 4. 15 - 31 days ago 5. More than 1 month but less than 3 months ago 6. More than 3 months ago but within the last 1 year 7. More than 1 year ago	Developed by UCT Metrics team; needs to be cognitively tested
Frequency	How often do these symptoms happen when/after using your phone or computer?	1. Never 2. Rarely 3. Often	Developed by UCT Metrics team; needs to be cognitively tested
Impact	How much do these symptoms affect your daily life (work/study/ relationships)?	1. Not At all 2. A little 3. Extremely	Developed by UCT Metrics team; needs to be cognitively tested

Key considerations:

- Linkages between mental health and technology use are challenging to measure because of the range of potential confounding variables, which may trigger or aggravate adverse mental health status.
- In cases where depression symptoms are persistent, and computer / phone use is a regular feature of day to day life, the question above on prevalence which seeks to establish temporal causal link between technology use and the onset of depression may be replaced with the question on perceived link with technology use seeking to establish aggravation of symptoms.

Body image and disordered eating outcomes

Research shows consistent links between social media use and body image concerns, with multiple meta-analyses finding associations between digital exposure, body dissatisfaction, and disordered eating outcomes [56]. Body dissatisfaction arises when there is a perceived gap between one's actual and ideal body image, which can contribute to disordered eating. Such outcomes include restrictive dieting, binge eating, purging behaviors, obsessive calorie counting, and an overemphasis on weight or shape. Importantly, social media can aggravate both existing body image concerns and disordered eating symptoms.

To assess body image concerns and disordered eating symptoms, several validated tools are available. The SCOFF questionnaire, developed in 1999 by Morgan, Reid, and Lacy, offers a brief screening with five yes/no questions, where a score above two indicates likely risk of an eating disorder. This is attached as **Annex 14**. For more detailed assessment, particularly when disordered eating outcomes are the study's main focus, more comprehensive instruments such as the Eating Attitudes Test (EAT-26) and the Eating Disorder Examination Questionnaire (EDE-Q) may be used. While these go beyond the scope of this toolkit, they remain important options for thorough evaluation.

Table 26. Survey questions for establishing a link between technology and disordered eating outcomes

Measurement element	Question	Response	Source
Perceived link between body image concerns and technology use (Aggravation)	Do you feel that your use of the phone or computer has an impact on how you feel about your body?	1. No impact 2. Positive impact on body image 3. Negative impact on body image	Developed by UCT Metrics team; needs to be cognitively tested
Perceived link between eating disorders and technology use (Aggravation)	Do you feel that your time on the phone or computer affects your eating habits or how you think about food?	1. No impact 2. Positive impact on body image 3. Negative impact on body image	Developed by UCT Metrics team; needs to be cognitively tested
Prevalence	[With reference to the SCOFF] Have you ever experienced these symptoms after using your phone or computer?	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested
	Do you feel worse about yourself after using your phone or computer?	1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested
Recency	When was the last time you experienced these symptoms after using your phone or computer?	1. Less than 24 hours ago 2. 2 - 7 days ago 3. 8 - 14 days ago 4. 15 - 31 days ago 5. More than 1 month but less than 3 months ago 6. More than 3 months ago but within the last 1 year 7. More than 1 year ago	Developed by UCT Metrics team

Measurement element	Question	Response	Source
Frequency	How often do these symptoms occur when/ after using your phone or computer?	1. Never 2. Rarely 3. Often	Developed by UCT Metrics team; needs to be cognitively tested
Impact	How much do these symptoms interfere with your daily life (work/study/ relationships)?	1. Not At all 2. A little 3. Extremely	Developed by UCT Metrics team; needs to be cognitively tested

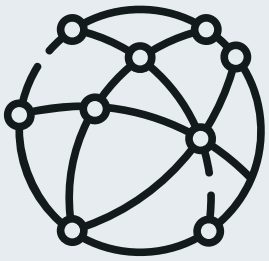
Key considerations:

- Linking technology use with eating disorders or body image issues is challenging to measure because of the range of potential confounding variables, which may trigger or aggravate adverse outcomes.
- In cases where eating disorders or body image symptoms are persistent, and computer / phone use is a regular feature of day to day life, the question above on prevalence which seeks to establish temporal causal link between technology use and the onset of these symptoms may be replaced with the question on perceived link with technology use seeking to establish aggravation of symptoms.

Self-injurious thoughts and behaviors

Self-injurious thoughts and behaviors (SITB)—including suicidal ideation, suicide attempts, and non-suicidal self-injury (NSSI)—refer to thoughts or actions of self-harm, with or without intent to die. SITB is a growing public health concern, particularly among adolescents and young adults. Evidence suggests that certain social media experiences—such as cyber victimization, problematic use, exposure to self-injurious content, and sexting—are associated with increased risks of SITB [66].

Measuring SITB is ethically and practically challenging. Sensitive questions about self-harm can cause distress, and stigma around mental health often discourages disclosure. In many LMIC settings, formal referral systems or accessible mental health services are limited or absent, so researchers may be unable to provide immediate support for participants identified as high-risk. Even with anonymized surveys or interviews, participants may withhold information or provide socially desirable responses due to fear of social, familial, or legal repercussions. These factors make it difficult to both ethically and reliably assess SITB in these contexts, highlighting the need for careful study design, clear communication, and provision of crisis resources wherever feasible. This is beyond the scope of this toolkit.



Annexes

Annex 1:
Survey questions for measuring attitudes towards violence

The Demographic and Health Survey (DHS) includes a single stem and leaf question on attitudes towards violence contained in the table below. To improve comprehension by respondents, a series of standalone questions are proposed. To add a digital component to this, two questions are recommended.

Question	Response
In your opinion, is a spouse justified in hitting or beating his wife if she goes out without telling him?	1. Yes 2. No
In your opinion, is a spouse justified in hitting or beating his wife if she neglects the children?	1. Yes 2. No
In your opinion, is a spouse justified in hitting or beating his wife if she argues with her spouse?	1. Yes 2. No
In your opinion, is a spouse justified in hitting or beating his wife if she refuses to have sex with spouse?	1. Yes 2. No
In your opinion, is a spouse justified in hitting or beating his wife if she burns the food?	1. Yes 2. No
In your opinion, is a spouse justified in hitting or beating his wife if she damages or breaks the mobile phone?	1. Yes 2. No
In your opinion, is a spouse justified in hitting or beating his wife if she posts videos or photos of herself on Facebook, Instagram or other social media platforms?	1. Yes 2. No

Annex 2:
Survey questions for measuring periodicity, perpetration, impact and response to digital violence.

Measurement element	Question	Response	Source
Recency	[If yes] When was the last time you received offensive and unwanted messages, calls, videos or photos?	1. Less than 24 hours ago 2. 2 - 7 days ago 3. 8 - 14 days ago 4. 15 - 31 days ago 5. More than 1 month but less than 3 months ago 6. More than 3 months ago, but within the last 1 year 7. More than 1 year ago	GSMA Consumer Survey 2023; cognitively tested in Kenya and Nigeria (2023-24)
Frequency	In the last 12 months, how often did you receive offensive or unwanted messages, calls, videos or photos?	1. Has never happened 2. Has happened once 3. Has happened 1-10 times 4. Has happened more than 10 times 5. Prefer not to say Alternatively, to simplify the following response option can be used: 1. Never 2. Rarely 3. Often	Domestic violence module; Tanzania demographic health survey (TDHS), 2022
Medium	The last time you received offensive or unwanted messages, calls, videos or photos, can you tell me how you received them? For example, through a phone call or on the internet.	**1. Standard mobile phone calls** **2. Voice calls on WhatsApp** or Telegram or Signal etc. **3. Video call on WhatsApp,** Telegram, Signal, Messenger and Facetime **4. SMS messages** **5. Text messages on WhatsApp/** **6. On social media** (e.g. Instagram, X/Twitter, Facebook, YouTube) **7. On a dating app/website** (Tinder, etc.) **8. On an online gaming app/website** (PubG, etc.) **9. Some other way,** specify _____	Adapted by UCT Metrics team from GKO 2021; cognitively tested in Kenya and Nigeria (2023-24)

Measurement element	Question	Response	Source
Perpetrator	Who was the person or people who sent you offensive or unwanted messages, calls, videos or photos? [Interview note: Select all mentioned]	1. Current spouse/partner/ boyfriend 2. Former spouse/partner/ boyfriend 3. Sister 4. Brother 5. Mother/step-mother 6. Father/step-father 7. Daughter/son 8. Mother-in-law 9. Father-in-law 10. Other relatives (aunts, uncles, cousins, grandparents) 11. Employer/someone at work 12. Teacher 13. Schoolmate/classmate 14. Someone met online 15. A stranger/unknown person 16. Others, specify_____ 17. Prefer not to say	TDHS, 2022; needs to be cognitively tested
Impact	Thinking about the last time you received offensive or unwanted messages, calls, videos or photos, how did you feel? [Enumerator note: Do not read out, select all mentioned]	1. Anger 2. Frustration 3. Humiliation 4. Fear 5. Sadness 6. Shame 7. Alone 8. Helpless 9. I did not feel anything 10. I don't know 11. Other specify _____	Developed by UCT Metrics team; needs to be cognitively tested

Measurement element	Question	Response	Source
Response/ Action taken	The last time you received offensive or unwanted messages, calls, videos or photos, what did you do? [Enumerator note: Do not read out response options. Ask 'anything else']	**No Action Taken** 1. Ignored the problem **Passive coping** 2. Logged off digital platform/closed app 3. Turned off internet/device 4. Removed/destroyed SIM **Restricted Own Behavior:** 5. Stopped using the internet for a period of time 6. Stopped using the digital platform/app **Active coping** 7. Deleted posts/messages/ comments from the other person **Changed device/app settings:** 8. Adjusted privacy or contact settings 9. Blocked or unfollowed the person 10. Restricted who could view posts or online content Responded Directly to the **Perpetrator** 11. Sent a message/called them - asking them to leave me alone **External help-seeking** 12. Told a family member 13. Told a friend 14. Reported the problem online 15. Reported or sought help from an offline protection agency (e.g., police, lawyer, social service organization such as NGO/CSO, or a religious leader) 16. Told a peer or colleague 17. Other (please specify: _____)	Parent question modified from GSMA; Response options are expanded from GKO (2021), Ofcom Pilot Online Harms Survey, TDHS (2022), The Economist (2021); UCT metric team cognitively tested in Kenya and Nigeria (2023-24)

Annex 3:
Survey questions for measuring the periodicity, perpetration, impact and response to online sexual violence

Measurement element	Question	Response	Source
Recency	If yes to any of the questions in Table 6] When was the last time [Insert harm] happened to you?	1. Less than 24 hours ago 2. 2 - 7 days ago 3. 8 - 14 days ago 4. 15 - 31 days ago 5. More than 1 month but less than 3 months ago 6. More than 3 months ago, but within the last 1 year 7. More than 1 year ago	Developed by UCT Metrics team
Frequency	In the last 12 months, how often did [insert harm] happen to you?	1. Never 2. Once 3. 1-10 times 4. More than 10 times Alternatively, to simplify the following response option can be used: 1. Never 2. Rarely 3. Often	Developed by UCT Metrics team; needs to be cognitively tested
Medium	The last time [insert harm] happened to you, can you tell me how? For example, through your mobile phone or the internet. [Enumerator note: Read out each option, select all that apply]	1. By mobile phone calls 2. By messages sent to your phone (SMS/text or MMS) 3. On Facebook, TikTok, Instagram, YouTube etc.) 4. By instant messaging (Facebook Messenger, WhatsApp, etc.) 5. On a dating app/website (Tinder etc.) 6. In an online game 7. Some other way, specify_____ 8. Prefer not to say	Adapted by UCT Metrics team from GKO 2021; cognitively tested in Kenya and Nigeria (2023-24)

Measurement element	Question	Response	Source
Perpetrator	Who was the person who did this [insert harm] to you? [Enumerator note: Probe “Anyone else?” and select all mentioned]	1. Current spouse/partner 2. Former spouse/partner 3. Sister/brother 3. Mother/step-mother 4. Father/step-father 5. Daughter/son 6. Mother-in-law 7. Father-in-law 8. Other relatives (aunts, uncles, cousins, grandparents) 9. Employer/someone at work 10. Teacher 11. Schoolmate/classmate 12. Someone met online, but with no personal connection 13. A stranger/unknown person 14. Others, specify_____ 15. Prefer not to say	TDHS, 2022; needs to be cognitively tested
Impact	Thinking about the last time [insert harm] happened to you, how did you feel? [Enumerator note: Do not read out, select all mentioned]	1. Anger 2. Frustration 3. Humiliation 4. Fear 5. Sadness 6. Shame 7. Alone 8. Helpless 9. I did not feel anything 10. I don’t know 11. Other specify _____	Developed by UCT Metrics team; needs to be cognitively tested

Measurement element	Question	Response	Source
Response/ Reaction	The last time [insert harm] happened to you, what did you do? [Enumerator note: Do not read out response options. Ask 'anything else']	**No action taken** 1. Ignored the problem **Close / shut down device** 2. Closed the app or browser window 3. Deleted any messages from the other person **Changing device/ app settings** 4. Changed my privacy/ contact settings 5. Blocked/ unfollowed the person 6. Restricted who could see posts/ online content **Self restricted behavior** 7. I stopped using the internet for a while 8. I stopped using the app **Responded to the person inflicting the harm** 9. Sent them a message to try to get them to leave me alone **Reported the problem** 10. Told family member 11. Told a friend 12. I reported the problem online 13. Sought help/reported to an offline harm protection agency (Police, lawyer, socio-service organization (NGOs/CSOs), religious leader) 98. Other specify__ ___	Parent question modified from GSMA; Response options are expanded from GKO (2021), Ofcom Pilot Online Harms Survey, TDHS (2022), The Economist (2021)

Annex 4:
Survey questions for measuring periodicity, perpetration, impact and response to doxing

Measurement element	Question	Response	Source
Recency	[If yes to the questions in Table 7] When was the last time [someone shared your personal private information without permission]?	1. Less than 24 hours ago 2. 2 - 7 days ago 3. 8 - 14 days ago 4. 15 - 31 days ago 5. More than 1 month but less than 3 months ago 6. More than 3 months ago, but within the last 1 year 7. More than 1 year ago	Adapted by UCT Metrics team from GSMA Consumer Survey 2023; cognitively tested in India, Kenya and Nigeria (2023-24)
Frequency	In the last 12 months, how often did [someone share your personal private information without permission]?	1. Never 2. Once 3. 1-10 times 4. More than 10 times Alternatively, to simplify the following response option can be used: 1. Never 2. Rarely 3. Often	Adapted by UCT Metrics team from Domestic violence module; Tanzania demographic health survey (TDHS), 2022
Medium	The last time [someone shared your personal private information without permission], where was the information shared? For example, in text messages or on the internet. [Enumerator note: Read out each option, select all that apply]	1. **Messaging platforms** (WhatsApp, Telegram, Messenger, Signal etc.) 2. **On social media** (eg. Instagram, X/Twitter, Facebook, YouTube) 3. **On a dating app/website** (Tinder, etc.) 4. **On an online gaming app/ website** (PubG, etc.) 5. **Some other way,** specify_____	Adapted by UCT metrics team from GKO 2021

Measurement element	Question	Response	Source
Perpetrator	Who was the person or people who [shared your personal or private information without permission] ? [Enumerator note: Probe “Anyone else?” and select all mentioned]	1. Current spouse/partner 2. Former spouse/partner 3. Sister/brother 3. Mother/step-mother 4. Father/step-father 5. Daughter/son 6. Mother-in-law 7. Father-in-law 8. Other relatives (aunts, uncles, cousins, grandparents) 9. Employer/someone at work 10. Teacher 11. Schoolmate/classmate 12. Someone met online, but with no personal connection 13. A stranger/unknown person 14. Others, specify_____ 15. Prefer not to say	Adapted by UCT metrics team from TDHS, 2022; needs to be cognitively tested
Impact	Thinking about the last time [someone shared your personal or private information without permission], how did you feel? [Enumerator note: Do not read out, select all mentioned]	1. Anger 2. Humiliation 3. Fear 4. Sadness 5. Curiosity 6. Shame 7. Alone 8. Helpless 9. Urge to attempt self-harm 10. I felt nothing special 11. I don’t know 12. Prefer not to say	Developed by UCT Metrics team; needs to be cognitively tested

Measurement element	Question	Response	Source
Response/ Reaction	The last time [someone shared your personal or private information without permission], what did you do? [Enumerator note: Do not read out response options. Ask 'anything else']	**No Action Taken** 1. Ignored the problem **Passive coping** 2. Logged off digital platform/ closed app 3. Turned off internet/device 4. Removed/destroyed SIM Restricted Own Behavior: 5. Stopped using the internet for a period of time 6. Stopped using the digital platform/app **Active coping** 7. Deleted posts/messages/ comments from the other person Changed device/app settings: 8. Adjusted privacy or contact settings 9. Blocked or unfollowed the person 10. Restricted who could view posts or online content Responded Directly to the Perpetrator 11. Sent a message/called them - asking them to leave me alone **External help-seeking** 12. Told a family member 13. Told a friend 14. Reported the problem online 15. Reported or sought help from an offline protection agency (e.g., police, lawyer, social service organization such as NGO/CSO, or a religious leader) 16. Told a peer or colleague 17. Other (please specify: __)	Parent question modified from GSMA; Response options are expanded from GKO (2021), Ofcom Pilot Online Harms Survey, TDHS (2022), The Economist (2021); UCT metric team cognitively tested in Kenya and Nigeria (2023-24)

Annex 5:
Survey questions for measuring the periodicity, perpetration, impact and response to physical violence related to technology use

Measurement element	Question	Response	Source
Recency	[If yes to any of the questions in Table 8] When was the last time someone ever verbally hurt or scolded you for breaking or damaging a mobile phone, computer or tablet?	1. Less than 24 hours ago 2. 2 - 7 days ago 3. 8 - 14 days ago 4. 15 - 31 days ago 5. More than 1 month but less than 3 months ago 6. More than 3 months ago, but within the last 1 year 7. More than 1 year ago	Developed by UCT Metrics team; needs to be cognitively tested
Frequency	In the last 12 months, how often did someone verbally hurt or scolded you for breaking or damaging a mobile phone, computer or tablet?	1. Never 2. Once 3. 1-10 times 4. More than 10 times Alternatively, to simplify the following response option can be used: 1. Never 2. Rarely 3. Often	Developed by UCT Metrics team; needs to be cognitively tested

Measurement element	Question	Response	Source
Perpetrator	Who was the person or people who verbally hurt or scolded you for breaking or damaging a mobile phone, computer or tablet? [Enumerator note: Probe "Anyone else?" and select all mentioned]	1. Current spouse/partner 2. Former spouse/partner 3. Sister/brother 3. Mother/step-mother 4. Father/step-father 5. Daughter/son 6. Mother-in-law 7. Father-in-law 8. Other relatives (aunts, uncles, cousins, grandparents) 9. Employer/someone at work 10. Teacher 11. Schoolmate/classmate 12. Someone met online, but with no personal connection 13. A stranger/unknown person 14. Others, specify_____ 15. Prefer not to say	Developed by UCT Metrics team; needs to be cognitively tested
Psychological impact	The last time someone verbally hurt or scolded you for breaking or damaging a mobile phone, computer or tablet, how did you feel? [Enumerator note: Do not read out, select all mentioned]	1. Anger 2. Frustration 3. Humiliation 4. Fear 5. Sadness 6. Shame 7. Alone 8. H elpless 9. I felt nothing special 10. I don't know 11. Other specify _____	Developed by UCT Metrics team; needs to be cognitively tested
Response/ Reaction	The last time someone verbally hurt or scolded you for breaking or damaging a mobile phone , computer or tablet, what did you do? [Enumerator note: Do not read out response options. Ask 'anything else']	**Reported the problem** 1. Told family member 2. Told a friend 3. Reported to harm protection agency (Police, lawyer, socio-service organization (NGOs/ CSOs), religious leader) **Sought help from** 4. Own family 5. Spouse's/partner's family 6. Friend 7. Neighbor 8. Doctor/medical personnel 9. Police 10. Lawyer 98. Other specify_____	Developed by UCT Metrics team; needs to be cognitively tested

Annex 6:
Survey questions for measuring the periodicity, perpetration, impact and response to physical violence related to technology use

Measurement element	Question	Response	Source
Recency	[If yes to any of the questions in Table 8] When was the last time someone physically hurt you for [insert action, i.e., breaking a phone, using the internet, etc.]?	1. Less than 24 hours ago 2. 2 - 7 days ago 3. 8 - 14 days ago 4. 15 - 31 days ago 5. More than 1 month but less than 3 months ago 6. More than 3 months ago, but within the last 1 year 7. More than 1 year ago	Developed by UCT Metrics team; needs to be cognitively tested
Frequency	In the last 12 months, how often did someone physically hurt you for [insert action, i.e., breaking a phone, using the internet, etc.]?	1. Never 2. Once 3. 1-10 times 4. More than 10 times Alternatively, to simplify the following response option can be used: 1. Never 2. Rarely 3. Often	Developed by UCT Metrics team; needs to be cognitively tested

Measurement element	Question	Response	Source
Perpetrator	Who was the person or people who physically hurt you for [insert action, i.e., breaking a phone, using the internet, etc.]?	1. Current spouse/partner 2. Former spouse/partner 3. Sister/brother 3. Mother/step-mother 4. Father/step-father 5. Daughter/son 6. Mother-in-law 7. Father-in-law 8. Other relatives (aunts, uncles, cousins, grandparents) 9. Employer/someone at work 10. Teacher 11. Schoolmate/classmate 12. Someone met online, but with no personal connection 13. A stranger/unknown person 14. Others, specify_____ 15. Prefer not to say	Developed by UCT Metrics team; needs to be cognitively tested
Health care seeking	The last time someone physically hurt you for [insert action, i.e., breaking a phone, using the internet, etc.], did you seek medical attention?	1. Yes 2. No	Adapted by UCT Metrics team from TDHS, 2022
	[If yes], Where did you seek care?	**Public sector** 1.National/Zonal/Specialized hospital 2. Regional referral hospital 3. Regional Hospital 4. District hospital 5. Health centre 6. Dispensary/Clinic 7. Other public sector (specify) **Private medical sector** 8. Specialized hospital 9. District hospital 10. Health Centre 11. Dispensary/Clinic 12. Other private medical sector (specify)_____	Adapted by UCT Metrics team from TDHS, 2022

Measurement element	Question	Response	Source
Psychological impact	The last time someone physically hurt you for [insert action, i.e., breaking a phone, using the internet, etc.], how did you feel? [Enumerator note: Do not read out, select all mentioned]	1. Anger 2. Frustration 3. Humiliation 4. Fear 5. Sadness 6. Shame 7. Alone and helpless 8. I felt nothing special 9. I don't know 10. Other specify _____	Developed by UCT Metrics team; needs to be cognitively tested
Physical impact	The last time someone physically hurt you for [insert action, i.e., breaking a phone, using the internet, etc.], what problems did it cause to your body? [Enumerator note: Do not read out, select all mentioned]	1. Pain in the body 2. Bruises or marks on the skin 3. Cuts 4. Broken or twisted bones/ joints 5. Hurt eye 6. Deep wound 7. Other specify	Developed by UCT Metrics team; needs to be cognitively tested
Response/ Reaction	The last time someone physically hurt you for [insert action, i.e., breaking a phone, using the internet, etc.], what did you do? [Enumerator note: Do not read out response options. Ask 'anything else']	**Reported the problem** 1. Told family member 2. Told a friend 3. Reported to harm protection agency (Police, lawyer, socio-service organization (NGOs/CSOs), religious leader) **Sought help from** 4. Own family 5. Spouse's/partner'sf amily 6. Friend 7. Neighbor 8. Doctor/medical personnel 9. Police 10. Lawyer 98. Other specify_____	Developed by UCT Metrics team; needs to be cognitively tested

Annex 7.
Survey questions for measuring the periodicity of false information

Measurement element	Question	Response	Source
Recency	[If yes, the above] When was the last time you read information like this?	1. Less than 24 hours ago 2. 2 - 7 days ago 3. 8 - 14 days ago 4. 15 - 31 days ago 5. More than 1 month but less than 3 months ago 6. More than 3 months ago, but within the last 1 year 7. More than 1 year ago	Developed by UCT Metrics team; needs to be cognitively tested
Frequency	In the last 12 months, how often have you read/seen any untrue information?	1. Never 2. Once 3. 1-10 times 4. More than 10 times Alternatively, to simplify the following response option can be used: 1. Never 2. Rarely 3. Often	Developed by UCT Metrics team; needs to be cognitively tested
Perpetrator	Who was the person who you heard this false information from? [Interview note: After each response probe "Anyone else?" Select all mentioned]	1. Current spouse/partner 2. Former spouse/partner 3. Sister/brother 3. Mother/step-mother 4. Father/step-father 5. Daughter/son 6. Mother-in-law 7. Father-in-law 8. Other relatives (aunts, uncles, cousins, grandparents) 9. Employer/someone at work 10. Teacher 11. Schoolmate/classmate 12. Someone met online, but with no personal connection 13. A stranger/unknown person 14. Others, specify_____ 15. Prefer not to say	Developed by UCT Metrics team; needs to be cognitively tested

Measurement element	Question	Response	Source
Medium	The last time you read or saw untrue information on the phone, where was it? [Enumerator note: Ask unprompted. Do not read out.]	1. **Phone call** (Traditional phone call, or voice call on WhatsApp, Telegram etc.) 2. **Video call** (on WhatsApp, Telegram, Signal, Facetime, etc.) 3. **Text message** (SMS, or on WhatsApp, Messenger, Telegram) 4. **Photo or video in chat** – (Photos or videos shared on WhatsApp, Telegram, Messenger, Signal etc.) 5. **Social media** (Facebook, YouTube, TikTok, Instagram, etc.) 6. **Websites** (news, online dating, banking, shopping) 7. **Searching the internet using AI**, such as Chat GPT, Google AI, WhatsApp AI search, Microsoft Co-pilot, etc. Add locally relevant examples) 8. **Other** – please say which one: _____	UCT Metrics team; cognitively tested New question, needs to be cognitively tested
Impact	Thinking about the last time you read or saw untrue information, how did it make you feel? [Enumerator note: Do not read out, select all mentioned]	1. Anger 2. Annoyed 3. Frustration 4. Humiliation 4. Fear 5. Sadness 6. Shame 7. Alone and helpless 8. I did not feel anything 9. I don't know 10. Confused/Unsure 11. Other specify _____	Developed by UCT Metrics team; needs to be cognitively tested

Measurement element	Question	Response	Source
Response/ Action taken	The last time you read or saw untrue information, what did you do? [Enumerator note: Do not read out response options. Ask 'anything else'] Have you ever reported something you saw or read on your phone — like a message, video, or social media post — because you believed it was untrue?	**No action taken** 1. Ignored the problem **Close / shut down device** 2. Closed the app or browser window 3. Deleted any messages from the other person **Changing device/ app settings** 4. Changed my privacy/ contact settings 5. Blocked/ unfollowed the person 6. Restricted who could see posts/ online content **Self restricted behavior** 7. I stopped using the internet for a while 8. I stopped using the app **Responded to the person inflicting the harm** 9. Sent a message to the person sharing false information or made a comment on the forum sharing false information. **Reported the problem** 10. Told family member 11. Told a friend 12. I reported the problem online 13. Sought help/reported to an offline harm protection agency (Police, lawyer, socio-service organization (NGOs/CSOs), religious leader) 98. Other specify_____ 1. Yes 2. No	Developed by UCT Metrics team; needs to be cognitively tested Developed by UCT Metrics team; needs to be cognitively tested

Annex 8:
Survey questions for measuring the privacy and data violations (recency, frequency, perpetrator, medium, impact and response)

Measurement element	Question	Response	Source
Recency	When was the last time this happened?	1. Less than 24 hours ago 2. 2 - 7 days ago 3. 8 - 14 days ago 4. 15 - 31 days ago 5. More than 1 month but less than 3 months ago 6. More than 3 months ago, but within the last 1 year 7. More than 1 year ago	Developed by the UCT Metrics team; cognitively tested in India, Kenya and Nigeria (2023-24)
Frequency	In the last 12 months, how often has this happened?	1. Never 2. Once 3. 1-10 times 4. More than 10 times Alternatively, to simplify the following response option can be used: 1. Never 2. Rarely 3. Often	Developed by the UCT Metrics team; cognitively tested in India, Kenya and Nigeria (2023-24)
Perpetrator	Who was the person that shared this information about you? Anyone else? [Interview note: Select all mentioned]	1. Current spouse/partner 2. Former spouse/partner 3. Sister/brother 3. Mother/step-mother 4. Father/step-father 5. Daughter/son 6. Mother-in-law 7. Father-in-law 8. Other relatives (aunts, uncles, cousins, grandparents) 9. Employer/someone at work 10. Teacher 11. Schoolmate/classmate 12. Someone met online, but with no personal connection 13. A stranger/unknown person 14. Others, specify_____ 15. Prefer not to say	Developed by UCT Metrics team; needs to be cognitively tested

Measurement element	Question	Response	Source
Medium	The last time this happened, did it happen through any of the following? [Enumerator note: Read out each option, select all that apply]	1. **Mobile phone calls** (Voice, WhatsApp) 2. **Video Call** (WhatsApp/FaceTime) 3. **Text message** (SMS, text, messenger WhatsApp MMS) 4. **Social media (** Facebook, TikTok, Instagram) 5. **Website** (online dating, banking, shopping) 6. **Government** services 7. **Other** ____ (please specify)	
Impact	Thinking about the last time this happened, how did you feel? [Enumerator note: Do not read out, select all mentioned]	1. Anger 2. Frustration 3. Humiliation 4. Fear 5. Sadness 6. Shame 7. Alone 8. Helpless 9. I did not feel anything 10. I don't know 11. Other specify _____	Developed by UCT Metrics team; needs to be cognitively tested
Response/ Action taken	The last time this happened to you, what did you do? [Enumerator note: Do not read out response options. Ask 'anything else']	**No action taken** 1. Ignored the problem **Close / shut down device** 2. Closed the app or browser window 3. Deleted any messages from the other person **Changing device/ app settings** 4. Changed my privacy/ contact settings 5. Blocked/ unfollowed the person 6. Restricted who could see posts/ online content **Self restricted behavior** 7. I stopped using the internet for a while 8. I stopped using the app **Responded to the person inflicting the harm** 9. Sent them a message to try to get them to leave me alone **Reported the problem** 10. Told family member 11. Told a friend 12. I reported the problem online 13. Sought help/reported to an offline harm protection agency (Police, lawyer, socio-service organization (NGOs/CSOs), religious leader) 98. Other specify_____	Parent question modified from GSMA; Response options are expanded from GKO (2021), Ofcom Pilot Online Harms Survey, TDHS (2022), The Economist (2021)

Annex 9:
Survey questions for measuring the digital fraud (recency, frequency, perpetrator, medium, impact and response)

Measurement element	Question	Response	Source
Recency	[If yes to the above] When was the last time this happened to you?	1.Less than 24 hours ago 2. 2 - 7 days ago 3. 8 - 14 days ago 4. 15 - 31 days ago 5. More than 1 month but less than 3 months ago 6. More than 3 months ago but within the last 1 year 7. More than 1 year ago	Developed by UCT Metrics team; cognitively tested in India, Kenya, and Nigeria (2023-24)
Frequency	In the last 12 months, how many times has your money been stolen over the phone or internet?	1. Never 2. Once 3. 1-10 times 4. More than 10 times Alternatively, to simplify the following response option can be used: 1. Never 2. Rarely 3. Often	Developed by UCT Metrics team; cognitively tested in India, Kenya, and Nigeria (2023-24)
Medium	The last time someone stole your money, did it happen through any of the following? [Enumerator note: Read out each option, select all that apply]	**Using:** **1.Voice calls** including traditional voice calls or voice calls on WhatsApp **2.Video calls** including WhatsApp, Skype, Telegram, Signal, Facetime **3. Text messages** including SMS, or on WhatsApp, Telegram, Signal, Messenger etc. **4. On social media**, such as Facebook, Instagram, Tik Tok etc. **5. Email**, including personal or business email **6. On a dating app/website** (Tinder, etc.) **6. Using more than one of these ways**– for example, using traditional mobile phone calls AND video calls. **7. Some other way,** specify_____	Developed by UCT Metrics team; needs to be cognitively tested

Measurement element	Question	Response	Source
Perpetrator	The last time your money was taken, who took the money?	1. Someone not known to me 2. Spouse/ partner 3. Someone in my family 4. Friend 5. Other specify_____	Developed by UCT Metrics team; cognitively tested in India (2023-24)
Impact	The last time your money was stolen, how much was taken?	Amount_____	Developed by UCT Metrics team; needs to be cognitively tested
Response/ Reaction	The last time your money was stolen, what did you do? [Enumerator note: Do not read out response options. Ask 'anything else']	**No action taken** 1. Ignored the problem **Stopped answering calls from strangers** 2. Stopped answering phone calls from strangers 3. Stopped answering WhatsApp calls from strangers **Close / shut down device** 4. Closed the app or browser window 5. Deleted any messages from the other person **Changing device/ app settings** 6. Changed my privacy/ contact settings 7. Blocked/ unfollowed the person 8. Restricted who could see posts/ online content **Self-restricted behavior** 9. I stopped using the internet for a while 10. I stopped using the app **Responded to the person inflicting the harm** 11. Sent them a message to try to get the money back **Reported the problem** 10. Told family member 11. Told a friend 12. I reported the problem online – for example by calling the government's cybercrime helpline or going to the cybercrime website 13. Sought help/reported to an offline harm protection agency (Police, lawyer, socio-service organization (NGOs/CSOs), religious leader) 98. Other specify_____	Developed by UCT Metrics team; needs to be cognitively tested

Annex 10:
Adapted Pittsburgh Sleep Quality Index (PSQI)

Measurement element	Question	Response	Source
Sleep quality	How would you rate your subjective sleep quality?	1. Very good 2. Somewhat good 3. Not good	Adapted by UCT Metrics team from Buysse 1989; needs to be cognitively tested
Sleep latency	In the last month, how long (in minutes) does it take you to fall asleep at night?	1. Less than 15 minutes 2. 15 to 30 minutes 3. 31 to 60 minutes 4. More than 60 minutes	
	During the past month, how often have you had difficulty falling asleep within 30 minutes?	1. Not at all 2. Less than once week 3. 1-2 times a week 4. >3 in a week	
Sleep duration	During the past month, how many hours of actual sleep did you get at night?	1. < 5 hours 2. 5-6 hours 3. 6-7 hours 4. >7 hours	
	On most nights, how often do you fall asleep and stay asleep while you are in bed?	1. Never 2. Rarely 3. Often	
Habitual Sleep Efficiency	During the past month, what time have you usually gone to bed at night?	___	
	During the past month, what time have you usually gotten up in the morning? [Enumerator note: Can calculate total sleep duration based on the above the responses]	___	
Use of sleep medication	During the past month, how often have you taken medicine (prescribed or "over the counter") to help you sleep?	1. Not during the past month 2. Less than once a week 3. Once or twice a week 4. Three or more times a week	
Daytime dysfunction	During the past month, how often have you had trouble staying awake while driving, eating meals, or engaging in social activity?	1. Not during the past month 2. Less than once a week 3. Once or twice a week 4. Three or more times a week	

Annex 11:
GAD -7 Questions

Survey question	Question response(s)
Over the last 2 weeks, how often have you been feeling nervous, anxious or on edge?	1. Not at all (0 points) 2. Several days (+1 point) 3. More than half the days (+2 points) 4. Nearly everyday (+3 points)
Over the last 2 weeks, how often have you been not being able to stop or control the worry?	1. Not at all (0 points) 2. Several days (+1 point) 3. More than half the days (+2 points) 4. Nearly everyday (+3 points)
Over the last 2 weeks, how often have you been worrying too much about different things?	1. Not at all (0 points) 2. Several days (+1 point) 3. More than half the days (+2 points) 4. Nearly everyday (+3 points)
Over the last 2 weeks, how often have you had trouble relaxing?	1. Not at all (0 points) 2. Several days (+1 point) 3. More than half the days (+2 points) 4. Nearly everyday (+3 points)
Over the last 2 weeks, how often have you been so restless that it is hard to sit still?	1. Not at all (0 points) 2. Several days (+1 point) 3. More than half the days (+2 points) 4. Nearly everyday (+3 points)
Over the last 2 weeks, how often have you been become easily annoyed or irritable?	1. Not at all (0 points) 2. Several days (+1 point) 3. More than half the days (+2 points) 4. Nearly everyday (+3 points)
Over the last 2 weeks, how often have you felt afraid as if something awful may happen?	1. Not at all (0 points) 2. Several days (+1 point) 3. More than half the days (+2 points) 4. Nearly everyday (+3 points)
Score interpretation: The following cut-offs correlate with level of anxiety severity: • Score 0-4: Minimal Anxiety • Score 5-9: Mild Anxiety • Score 10-14: Moderate Anxiety • Score greater than 15: Severe Anxiety Based on meta-analysis, some experts have recommended considering using a cut-off of 8 in order to optimize sensitivity without compromising specificity.	

Annex 12:
Bergan Social Media Addiction Scale

	Survey Question	Response*
Salience	During the past year, how often have you spent a lot of time thinking about social media or planned use of it?	1. Never 2. Rarely 3. Often
Tolerance	During the past year, how often have you felt an urge to use social media more and more?	1. Never 2. Rarely 3. Often
Mood modification	During the past year, how often have you used social media to forget about personal problems?	1. Never 2. Rarely 3. Often
Relapse	During the past year, how often have *you tried to cut down on the use of social media without success?*	1. Never 2. Rarely 3. Often
Withdrawal	During the past year, how often have you become restless or troubled if you have been prohibited from using social media?	1. Never 2. Rarely 3. Often
Conflict	During the past year, how often have *you used social media so much that it has had a negative impact on your job/studies?*	1. Never 2. Rarely 3. Often

*Likert scale response options have been modified for use in low literate populations from the original 5 point scale of agreement (1 = Very rarely, 2 = Rarely, 3 = Sometimes, 4 = Often, 5 = Very often)

Annex 13:
PHQ-9 validated depression questionnaire

Survey question	Question response(s)
Over the last two weeks, how often have you been bothered by the following problems?	
Little interest or pleasure in doing things	1. Not at all (0 points) 2. Several days (+1 point) 3. More than half the days (+2 points) 4. Nearly everyday (+3 points)
Feeling down, depressed or hopeless	1. Not at all (0 points) 2. Several days (+1 point) 3. More than half the days (+2 points) 4. Nearly everyday (+3 points)
Trouble falling asleep or sleeping too much	1. Not at all (0 points) 2. Several days (+1 point) 3. More than half the days (+2 points) 4. Nearly everyday (+3 points)
Feeling tired or having little energy	1. Not at all (0 points) 2. Several days (+1 point) 3. More than half the days (+2 points) 4. Nearly everyday (+3 points)
Poor appetite or over eating	1. Not at all (0 points) 2. Several days (+1 point) 3. More than half the days (+2 points) 4. Nearly everyday (+3 points)
Feeling bad about yourself- or that you are a failure or have let yourself or your family down	1. Not at all (0 points) 2. Several days (+1 point) 3. More than half the days (+2 points) 4. Nearly everyday (+3 points)
Trouble concentrating on things, such as watching television or reading the newspaper	1. Not at all (0 points) 2. Several days (+1 point) 3. More than half the days (+2 points) 4. Nearly everyday (+3 points)
Moving or speaking so slowly that other people could have noticed. Or the opposite- being so fidgety or restless that you have been moving around a lot more than usual	1. Not at all (0 points) 2. Several days (+1 point) 3. More than half the days (+2 points) 4. Nearly everyday (+3 points)
Thoughts that you would be better off dead, or of hurting yourself in some way.	1. Not at all (0 points) 2. Several days (+1 point) 3. More than half the days (+2 points) 4. Nearly everyday (+3 points)

Annex 14:
SCOFF Questionnaire

Survey question	Question response(s)
Do you make yourself sick because you feel uncomfortably full?	1. Yes 2. No
Do you worry you have lost control over how much you eat?	1. Yes 2. No
Have you recently lost one stone (≈14 lbs / 6.35 kg) in a 3-month period?	1. Yes 2. No
Do you believe yourself to be fat when others say you are too thin?	1. Yes 2. No
Would you say that food dominates your life?	1. Yes 2. No

References

REFERENCES

1. Kuss, D.J., *Online harms: Problematic technology use is a public health concern and requires a multistakeholder approach.* Addictive Behaviors Reports, 2025 Mar 29. **21**.
2. Daniel, R., H. Austin, and R. Paula. *Replicating the Mobile Revolution* 2024 [cited 2025 18/09]; Available from: https://www.csis.org/analysis/replicating-mobile-revolution.
3. Livingstone, S. and P.K. Smith, *Annual Research Review: Harms experienced by child users of online and mobile technologies: the nature, prevalence and management of sexual and aggressive risks in the digital age*. 2014.
4. UNICEF. *COVID-19 and its implications for protecting children online*. 2020 [cited 2025 18/09]; Available from: https://www.unicef.org/sites/default/files/2020-04/COVID-19-and-Its-Implications-for-Protecting-Children-Online.pdf.
5. Bank, W. *World Development Report 2021: Data for better lives*. 2021 [cited 2025 18/09]; Available from: https://www.worldbank.org/en/publication/wdr2021.
6. Twenge, J.M. and W.K. Campbell, *Associations between screen time and lower psychological well-being among children and adolescents: Evidence from a population-based study.*
7. Stevens, F., et al., *Women are less comfortable expressing opinions online than men and report heightened fears for safety: Surveying gender differences in experiences of online harms*. 2024/03/27.
8. Women, U. *Online and ICT facilitated violence against women and girls during COVID-19*. 2020 [cited 2025 18/09]; Available from: https://www.unwomen.org/en/digital-library/publications/2020/04/brief-online-and-ict-facilitated-violence-against-women-and-girls-during-covid-19.
9. Matthew, S. and B. Kalvin. *The State of Mobile Internet Connectivity*. 2024 [cited 2025 18/09]; Available from: https://www.gsma.com/r/wp-content/uploads/2024/10/The-State-of-Mobile-Internet-Connectivity-Report-2024.pdf.
10. Scott, K., et al., *Freedom within a cage: how patriarchal gender norms limit women's use of mobile phones in rural central India.*
11. Niskier, S.R., et al., *Adolescent Screen Use: Problematic Internet Use and the Impact of Gender.* Psychiatry Investigation, 2024 Jan 12. **21**(1).
12. WHO, U.W.a. *TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN:TAKING STOCK OF EVIDENCE AND DATA COLLECTION*. 2023 [cited 2025 18/09]; Available from: https://www.unwomen.org/sites/default/files/2023-04/Technology-facilitated-violence-against-women-Taking-stock-of-evidence-and-data-collection-en.pdf.
13. Stacey Fisher , C.B., Deirdre Hennessy , Tony Robertson , Alastair Leyland , Monica Taljaard , Claudia Sanmartin , Prabhat Jha , John Frank , Jack V. Tu , Laura C. Rosella , JianLi Wang , Christopher Tait , and Douglas G. Manuel, *International population-based health surveys linked to outcome data: A new resource for public health and epidemiology* Health Reports, 2020.
14. Joustra, A., L. Quinn, and V. Walker, *Recognition, prevention and management of 'digital harm'.* Archives of Disease in Childhood - Education and Practice, 2024-06-01. **109**(3)
15. Claire, W. and D. Hossein. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. 2017 [cited 2025 18/09]; Available from: https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html.
16. Daniel, S., *A Taxonomy of Privacy.* Law Review, 2006. **154**.

17. WHO. *Guidelines on physical activity, sedentary behaviour and sleep for children under 5 years of age*. 2019 [cited 2025 18/09]; Available from: https://www.who.int/publications/i/item/9789241550536.
18. Scott, K., Ummer, O., Sarangi, A., Mackenzie, C., Obi, I, Abdullahi, B.U., Nchogu, S., Chakravarthy, V, Taluja, Z. & LeFevre, A.E. & the Evidence for Digital Transformation research team., *Measuring digital access and use in global surveys: Findings from cognitive interviews to enhance surveys in India, Kenya and Nigeria*.
19. Taluja, Z., Sarangi, A., Mishra, P., Verma, C.P., Sharma, M., Ummer, O., Khanna, A., Chamberlain, S., Krishnaraj, P., Hudda, M.S., LeFevre, A.E. & Scott, K., *Yes, but please speak in Hindi. What does the question mean?": Cognitive interviews to enhance measurement of digital access and use in rural north India.*
20. L, H., et al. *Technology-facilitated gender-based violence: What is it, and how do we measure it?,*. 2018 [cited 2025 18/09]; Available from: https://www.icrw.org/publications/technology-facilitated-gender-based-violence-what-is-it-and-how-do-we-measure-it/.
21. WHO. *Ethical and safety recommendations for intervention research on violence against women. Building on lessons from the WHO publication Putting women first: ethical and safety recommendations for research on domestic violence against women*. 2016 [cited 2025 18/09]; Available from: https://iris.who.int/bitstream/handle/10665/251759/9789241510189-eng.pdf#page=14.14.
22. SVRI. *Ethical and Safety Guidelines for Research on Gender-Based Violence*. 2018 [cited 2025 18/09]; Available from: https://www.svri.org/sites/default/files/attachments/2018-05-09/Annex%203%20Ethical%20%26%20Safety%20Guidelines_0.pdf.
23. PATH. *Ethical Considerations for Researching Violence Against Women: A practical guide for researchers and activists*. 2005 [cited 2025 18/09]; Available from: https://www.path.org/our-impact/resources/researching-violence-against-women-a-practical-guide-for-researchers-and-activists/.
24. WHO, *Public Health Implications of Excessive Use of the Internet,Computers, Smartphones and Similar Electronic Devices Meeting report*. 2014. p. 151.
25. Best, P., R. Manktelow, and B. Taylor, *Online communication, social media and adolescent wellbeing: A systematic narrative review.* Children and Youth Services Review, 2014/06/01. **41**.
26. UNODC. *UNODC Teaching Module Series: Cybercrime*. [cited 2025 18/09]; Available from: https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-12/key-issues/cyberbullying.html.
27. Equality, E.I.f.G. *Revenge porn*. 2017 [cited 2025 18/09]; Available from: https://eige.europa.eu/publications-resources/thesaurus/terms/1459?language_content_entity=en.
28. UK, G. *Upskirting: know your rights*. 2019 [cited 2025 18/09]; Available from: https://www.gov.uk/government/news/upskirting-know-your-rights.
29. N, H. and B. G, *Image-Based Sexual Abuse Perpetration: A Scoping Review - PubMed*. Trauma, violence & abuse, 2024 Dec. **25**(5).
30. Ray, A., N. Henry, and N.H. Alana Ray, *Sextortion: A Scoping Review.* Trauma, Violence, & Abuse, 2025-1.
31. Now, E., *Deepfake Image-Based Sexual Abuse, Tech-Facilitated Sexual Exploitation and The Law*. 2023. p. 9.
32. Karasavva, V., et al., *Putting the Y in cyberflashing: Exploring the prevalence and predictors of the reasons for sending unsolicited nude or sexual images.* Computers in Human Behavior, 2023/03/01. **140**.

33. Now, E., *Ending Online Sexual Exploitation and Abuse of Women and Girls: A Call for International Standards*. p. 70.
34. Commissioner, e. *Doxing*. 2025 [cited 2025 18/09]; Available from: https://www.esafety.gov.au/industry/tech-trends-and-challenges/doxing.
35. Women, U. *Creating safe digital spaces free of trolls, doxing, and hate speech*. 2024 [cited 2025 24/09]; Available from: https://www.unwomen.org/en/articles/explainer/creating-safe-digital-spaces-free-of-trolls-doxing-and-hate-speech.
36. Now, E. *New research brief: Doxing, digital abuse and the law*. 2024 [cited 2025 24/09]; Available from: https://equalitynow.org/news/news-and-insights/new-research-brief-doxing-digital-abuse-and-the-law/.
37. Karakurt, G. and K.E. Silver, *Emotional abuse in intimate relationships: The role of gender and age*. Violence and victims, 2013. **28**(5).
38. Ness, S., *A narrow focus in research on emotional abuse: A scoping review of definitions and descriptions on emotional abuse in research on child welfare and social work*. Child & Family Social Work, 2023/05/01. **28**(2).
39. Alanazi, S., et al., *Exploring deepfake technology: creation, consequences and countermeasures*. Human-Intelligent Systems Integration 2024 6:1, 2024-09-18. **6**(1).
40. Office, I.C.s., *Overview of Data Protection Harms and the ICO's Taxonomy*. 2022. p. 13.
41. OECD. *Online Identity Theft*. 2009 [cited 2025 18/09]; Available from: https://www.oecd.org/en/publications/online-identity-theft_9789264056596-en.html.
42. Lords, H.o., *Surveillance: Citizens and the State*. 2009. p. 130.
43. DevX. *Hacking*. 2023 [cited 2025 24/09]; Available from: https://www.devx.com/terms/hacking/.
44. Brenncke, M. and M. Brenncke, *A Theory of Exploitation for Consumer Law: Online Choice Architectures, Dark Patterns, and Autonomy Violations*. Journal of Consumer Policy 2023 47:1, 2023-12-15. **47**(1).
45. Pillay, N., et al., *Translating the consent form is the tip of the iceberg: using cognitive interviews to assess the barriers to informed consent in South African health facilities*. Sexual and Reproductive Health Matters, 2023-12-01. **31**(4).
46. A, L., et al., *Preferences for onward health data use in the electronic age among maternity patients and providers in South Africa: a qualitative study - PubMed*. Sexual and reproductive health matters, 2023 Dec. **31**(4).
47. Elliot, M., et al., *Dictionary of Privacy, Data Protection and Information Security*. 2024/07/16.
48. consulting, I. *General Data Protection Regulation (GDPR), Art. 4 GDPR Definitions*. [cited 2025 24/09]; Available from: https://gdpr-info.eu/art-4-gdpr/.
49. Favaretto, M., et al., *Big Data and discrimination: perils, promises and solutions. A systematic review*. Journal of Big Data 2019 6:1, 2019-02-05. **6**(1).
50. EU. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. 2016 [cited 2025 19/09]; Available from: https://gdpr-info.eu/.

51. Examiners, A.o.C.F. *What Is Fraud?* [cited 2025 18/09]; Available from: https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud.

52. Longevity, S.C.o., *Framework for a taxonomy of fraud*. 2015. p. 40.

53. Kipngetich, A., et al., *A review of online scams and financial frauds in the digital age*. GSC Advanced Research and Reviews, 2025. **22**(1).

54. INTERPOL. *INTERPOL Financial Fraud assessment: A global threat boosted by technology*. 2024 [cited 2025 24/09]; Available from: https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology.

55. Devi, K.A. and S.K. Singh, *The hazards of excessive screen time: Impacts on physical health, mental health, and overall well-being.* Journal of Education and Health Promotion, 2023 Nov 27. **12**(1).

56. O, A., et al., *Social media use, mental health and sleep: A systematic review with meta-analyses - PubMed*. Journal of affective disorders, 12/15/2024. **367**.

57. MC, C.-A., et al., *Effects of remote learning during the COVID-19 lockdown on children's visual health: a systematic review - PubMed*. BMJ open, 08/03/2022. **12**(8).

58. P, C., et al., *Associations of screen work with neck and upper extremity symptoms: a systematic review with meta-analysis - PubMed*. Occupational and environmental medicine, 2019 Jul. **76**(7).

59. Wang, J., et al., *Mobile Phone Use and The Risk of Headache: A Systematic Review and Meta-analysis of Cross-sectional Studies.* Scientific Reports, 2017 Oct 3. **7**.

60. DJ, B., et al., *The Pittsburgh Sleep Quality Index: a new instrument for psychiatric practice and research - PubMed.* Psychiatry research, 1989 May. **28**(2).

61. AL, S. and W. JS, *Digital eye strain: prevalence, measurement and amelioration - PubMed.* BMJ open ophthalmology, 04/16/2018. **3**(1).

62. D, T.-P., et al., *Conceptualising social media addiction: a longitudinal network analysis of social media addiction symptoms and their relationships with psychological distress in a community sample of adults - PubMed.* BMC psychiatry, 07/13/2023. **23**(1).

63. W, W., H. L, and Y. F, *Social anxiety and problematic social media use: A systematic review and meta-analysis - PubMed.* Addictive behaviors, 2024 Jun. **153**.

64. S, C., H. CC, and H. K, *Social Media and Depression Symptoms: a Meta-Analysis - PubMed.* Research on child and adolescent psychopathology, 2021 Feb. **49**(2).

65. K, K., S. RL, and W. JB, *The PHQ-9: validity of a brief depression severity measure - PubMed.* Journal of general internal medicine, 2001 Sep. **16**(9).

66. Nesi, J., et al., *Social Media Use and Self-Injurious Thoughts and Behaviors: A Systematic Review and Meta-Analysis*. Clinical psychology review, 2021 May 8. **87**.

NOTES

Measuring Digital Harms in Low and Middle-Income Countries

A guide for inclusive research and design

2x Digital

UNIVERSITY OF CAPE TOWN
IYUNIVESITHI YASEKAPA • UNIVERSITEIT VAN KAAPSTAD

School of Public Health
Departement Openbare Gesondheid
Isikolo Sempilo Yoluntu
UNIVERSITY OF CAPE TOWN

YORK U

JOHNS HOPKINS
BLOOMBERG SCHOOL
of PUBLIC HEALTH