‘Ought’ should not assume ‘Can’ ...

Basic Capabilities in Cybersecurity to Ground Sen’s Capability Approach

Partha Das Chowdhury
University of Bristol,
Bristol, UK
partha.daschowdhury@bristol.ac.uk

Karen V. Renaud
University of Strathclyde,
Glasgow, UK
University of South Africa, RSA, Abertay University, UK,
Rhodes University, RSA
karen.renaud@strath.ac.uk

ABSTRACT

We inhabit a ‘digital first’ society, which is only viable if everyone, regardless of ability and capacity, is able to benefit from online offerings in a safe and secure way. However, disabled individuals, people living under oppressive regimes, elderly citizens and individuals fleeing conflict can be excluded, because they might not have the opportunity to implement cybersecurity hygiene measures. To reduce this potential exclusion, it is crucial to make all users’ situated realities focal variables in policy debates and provisioning efforts. This requires a validated set of basic minimum capabilities which reflect individuals’ diverse personal and social realities. In this paper, we report on a scoping literature review intended to reveal the state of play with respect to capabilities-related research in the cyber domain. We motivate our initial focus on the over 65s for this investigation. We used advice from online government cybersecurity advisories to arrive at a set of five recommended cybersecurity hygiene tasks. These fed into a survey with sixty senior citizens to elicit the barriers they could envisage someone of their age encountering, in acting upon cybersecurity hygiene advice. The final deliverable is a candidate list of *basic capabilities (cybersecurity)* for seniors. This enables us to start measuring security and privacy poverty, an essential step in recognising and mitigating exclusion, as well as informing threat modelling efforts.

CCS CONCEPTS

• **Security and privacy** → **Social network security and privacy**; • **Human-centered computing** → **Accessibility**; **Accessibility theory, concepts and paradigms**; • **Social and professional topics** → **User characteristics**; **Seniors**; **People with disabilities**.

KEYWORDS

capability approach, cybersecurity hygiene, list of basic capabilities

ACM Reference Format:
Partha Das Chowdhury and Karen V. Renaud. 2023. ‘Ought’ should not assume ‘Can’ ...: **Basic Capabilities in Cybersecurity to Ground Sen’s Capability Approach**. In *New Security Paradigms Workshop (NSPW ’23), September 18-21, 2023 in Segovia, Spain.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
NSPW ’23, September 18-21, 2023, Segovia, Spain
© 2023 Association for Computing Machinery.
ACM ISBN 000. . . $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

The Internet is a public good, the ubiquity and cost effectiveness of which has led many governments and organisations to adopt a ‘digital first’ strategy in service delivery. Citizens should: (1) have access to online services (i.e., device and internet access), (2) be able to interact with them (i.e., have knowledge and abilities), and (3) do so safely and securely (i.e., practice cybersecurity hygiene). All of these are critical in unlocking significant human rights [1], but none can be guaranteed. It is important not to assume that mere availability of security tools and wide dissemination of security advice will be sufficient for citizens to exercise these rights: i.e., ‘*ought*’ should not assume ‘*can*’.

The essential enabler is *capability*, without which people **cannot** follow cybersecurity hygiene advice. A number of factors compromise capability, including age-related infirmities, limited education, low literacy, disabilities, gender and socio-economic circumstances [2–6]. At present, more capable individuals benefit from the protection afforded by cybersecurity hygiene measures, but less capable individuals remain vulnerable online.

The pertinent question is how to ensure that everyone, including the currently excluded, can participate safely and securely in our ‘digital first’ society, regardless of level of capability. Recent research [7] concluded that the current approach of building systems privileging utilitarian usability is inadequate to capture human *needs* in their diversity. Utility cannot, and is not, meant to capture human *needs* [8]. The reality is that human (in)dispositions are not generally the focus of system designers and application developers [9]. The current *status quo* of inherently exclusionary systems is the consequence. Das Chowdhury *et al.* [7] argue that *capability approach*, as a methodological foundation of how protection mechanisms are conceived and developed, does indeed have the ability to highlight the *needs* of diverse individuals and the potential to reduce exclusionary practices.

This proposed paradigm shift calls for serious consideration of how the *capability approach* might be realised in the cyber domain. In this paper, we focus on isolating and identifying *basic capabilities (cybersecurity)*: the minimum provisions an individual should have to achieve a basic level of cybersecurity hygiene. This research is the first systematic exposition of the methodological advance proposed by Das Chowdhury *et al.* [7].

Section 2 argues the need for a list of *basic capabilities (cybersecurity)*. Then, as shown in Figure 1, Section 3 reports on a scoping

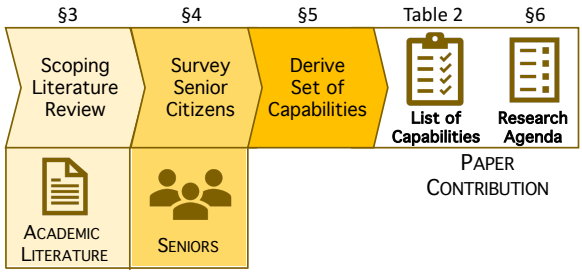

Figure 1: Structure of this Paper

review of the cyber literature's treatment of capabilities. We found borderline engagement with the *capability approach*. Section 4 explains how we surveyed senior citizens to isolate the capabilities needed to carry out specific recommended cybersecurity hygiene tasks. Section 5 reports on our findings and provides a final list of *basic capabilities (cybersecurity)* (Table 2 and Figure 6). Section 6 outlines a research agenda based on our findings and Section 7 concludes. The contributions of this paper are:

Contribution 1: A candidate list of *basic capabilities (cybersecurity)* for senior citizens, shown in Table 2. These pertain to the *capabilities* seniors should possess to carry out recommended cybersecurity hygiene tasks. Our list likely needs to be refined, and used to provide a foundation for future research in this area. This list enables the development and deployment of equitable, secure and privacy-protective interventions.

Contribution 2: A *research agenda* to improve inclusion by addressing security and privacy poverty — individuals without the basic minimum are poor in protection mechanisms they ought to be able to use, in order to securely participate in a 'digital first' society. For example, an elderly citizen with age-related vision loss does not have the capability to use multifactor authentication (MFA) mechanisms that require him/her to see the code and enter it. That is an absence of *basic capability (cybersecurity)* for the said individual if MFA is mandated. Such absence of *capabilities* can be used to measure exclusion, security & privacy poverty. On a general note, measuring poverty as absence of *basic capabilities* is considered methodologically sound in areas engaged in provisioning of public goods such as food and healthcare [10]. The foundation to do so in cybersecurity is a novel contribution of our work.

2 CAPABILITY APPROACH & THE NEED FOR BASIC CAPABILITIES (CYBERSECURITY)

2.1 The Capability Approach

Capability approach was first outlined by Sen while drawing out the limitations of the utilitarian & Rawlsian approaches to welfare [11]. *Capability approach* is a framework of thought with individual diversity and freedom at its core. There are two fundamental ingredients in *capability approach* as:

- **Capabilities:** the freedom a person has to choose the life they can lead and value.
- **Functioning:** *beings* and *doings* of a person. For example, securely accessing one's own online bank account is 'a functioning'.

Capabilities are the opportunities an individual has, whereas *functioning* is a set of actions the individual carries out in his/her life. The capability approach framework is a departure from a resource-oriented view — mere possession of a good is not sufficient for an individual to be able to benefit from it. For example, a bicycle is of no use to a person who does not have the physical ability to ride it. A *capability approach* based evaluation considers this diversity in physical ability of individuals while assessing individuals' opportunity to achieve the *functioning* of being mobile.

Human diversity is central to the framework and *capability approach* and points to the information that is necessary to achieve this inter-personal welfare comparison (the welfare a bicycle brings to a person who cannot ride vs. someone who can ride). While *capabilities* refer to opportunities an individual has, there is a subset of *capabilities* which refers to the ability to do some basic things. If an individual is able to do those basic things, they can achieve or unlock better things. *Basic capabilities* are a subset of all the *capabilities*. For example, a *basic capability* for a vision-impaired person is to go out and get around in the same way as a sighted person can.

> *"Basic capability means the freedom to do certain basic things, for example the ability to read and write is a* ***basic capability*** *in certain jurisdictions. A literate person can then unlock higher* capabilities*. They can help 'in deciding on a cut-off point for the purpose of assessing poverty and deprivation' "* [12, p. 109].

An example from mobility can help to convey the notion of *basic capability*. A *basic capability* for an abled individual with good eye-sight is to be able to use their eyes to cross busy roads safely. This led to the provisioning of zebra crossings and push buttons to stop traffic. However, for individuals without vision or partial sight, the ability to avail themselves of a zebra crossing without seeing, is a basic need if they are to go out. A recognition of this, as a *basic capability*, led to the provisioning of audible pedestrian push buttons and tactile pavings on top of zebra crossings. Such provisioning enables people without eye sight not only to be mobile but to do this in a manner compatible with human dignity. Universal healthcare is another example where equitable access empowers citizens to live the life they value [10]. In countries with high infant mortality, many children do not have the freedom to be able to live after being born [13]. There, it becomes pertinent to define *ability to live after being born* as a *basic capability* that everyone should have. A contextual list of *basic capabilities* is founded upon upon an assessment of personal and societal factors that negatively influence the freedom to do certain things.

Defining *basic capability*, explicitly incorporating specific deprivations, drives the need for policy change and consequent service provisioning. We consider the term 'policy' to mean developing regulatory instruments at the national/internal level. Situating the *capability approach* has been commented upon by Das Chowdhury *et al.* [7] — a regulatory need would ensure applications are developed keeping disadvantaged groups in mind. There are parallels in other domains [14].

2.2 Basic Capabilities (Cybersecurity)

A list of *basic capabilities* is a fundamental ingredient in the implementation of the *capability approach* for equitable provisioning of public goods. The original formulation of *capability approach* uses the term *basic capabilities*; we use *basic capabilities (cybersecurity)* where appropriate to delineate our context. We now draw upon some user studies as illustrative examples to emphasise the need for a list of *basic capabilities* in the cybersecurity context. They are illustrative of the fact that they study how humans respond to certain situations and goods, in this case cybersecurity hygiene tasks. They stop short of capturing the opportunities individuals have to respond in an appropriate manner.

A study to understand how email content and age of the Internet user influences detection of phishing emails was carried with 100 young (M = 21.7 years) and 58 older (M = 61.7 years) users [15]. The study revealed that older users are more susceptible to phishing emails. Quantitative empirical insights about how humans respond to phishing emails is significant but stops short of capturing the deprivations that might contribute to their susceptibility. Nevertheless, the influence of age, gender and appropriate training on the ability to detect phishing and take preventive action is being argued in a recent systematisation effort [16]. For example, indispositions can prevent people from noticing phishing warnings (impaired vision), to remember mitigation actions (poor memory), and perform them (dexterity or dyslexia). Framing secure passwords is widely recommended. A user study to evaluate the ability to create acceptable passwords showed that the rules are onerous. Most could not create secure passwords [17]. Renaud *et al.* [18] found that the endowment effect could deter adoption of more secure password creation methods.

While there are expectations (among system designers) that users should behave in a manner the security policy expects them to [19], a nuanced understanding of other disciplines tells us that such assumptions are contrary to human beings and doings [20]. For example, there is a gap in studying the password usage ability of dyslexic individuals [5]. Sim *et al.* [21] report that older adults with disabilities are often neglected in security design deliberations.

Prior work posits that the *capability approach* can complement the social model of disability [22]. Together, they can effectively assess the reduced opportunities that less abled individuals have in participating in the digital world. The field of cybersecurity needs to explicitly capture human deprivations, beings and doings because individuals' ability to use any protection mechanism is influenced by these factors.

Defining *basic capabilities (cybersecurity)* means making such intrinsic indispositions focal variables in policy making, which, in turn, will determine subsequent provisioning of online protection mechanisms. For example, a regulatory need for implementing *basic capability to use MFA with arthritic hands* can enable pervasive provisioning of mechanisms to afford this activity. Plurality of focal variables opens the digital space for diverse individuals and enables them to participate in a 'digital first' society compatible with human dignity. A contextual list of *basic capabilities (cybersecurity)* has the potential to make security accessible and inclusive by design [6] rather than *ad-hoc* — limited by the imagination and experiences of the system designer.

3 SCOPING REVIEW

We reviewed related literature to provide a snapshot of research in the cyber domain where user capabilities or the capability approach are mentioned. We searched SCOPUS, IEEE, USENIX, ACM, OpenAlex, World of Science, and Crossref concluding with a final Google Scholar search to ensure comprehensiveness. Figure 2 (unshaded boxes) depicts the search parameters and process. Subsequently, we identified two seminal papers in our corpus (cited 310 [23] and 7848 [24] times). We subsequently used Google Scholar to search for cyber-related papers that cited these two papers, to add these to our corpus. See Figure 2 (shaded boxes).

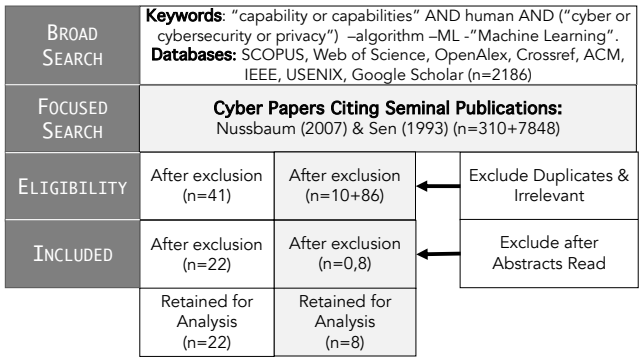

Figure 2: PRISMA of Literature Searches (Shaded Boxes = Citations of Seminal Papers)

Exclusion Criteria:

We were left with a total of 30 papers to support analysis that explicitly discussed *capabilities* in the cyber domain, satisfying the following criteria:

- The paper should explicitly mention *capabilities*, or
- The paper should report on an application of *capability approach*.

Analysis:

We reviewed and recorded the following data items concerning capabilities in each paper:

- **Q1:** How are capabilities discussed in the security and privacy research literature?
- **Q2:** Do authors propose any solutions for people with capability issues?
- **Q3:** What are the criticisms of the capability approach?

The researchers independently reviewed the papers ensuring consistency and reliability of the analysis process.

3.1 Q1: Capabilities

3.1.1 *Capabilities in General Terms:*

There are studies that explore the role of information and communication technologies (ICT) to augment human *capabilities*. ICT enabled positive transformation among urban informal settlement communities in South Africa [25] while living amidst their other precarities. A notable narrative method based study [26] conducted

in Pakistan outlines the *capabilities* ICTs enable. A related ethnographic study [27] conducted among populations from two areas in Trinidad highlight that usage of social networking sites by individuals is influenced by what they *value*. The pertinent gap in these studies, from the perspective of the *capability approach*, is an understanding of the conversion factors that drive or act as barriers to the use of ICTs. For example, an ethnographic study in Homa Bay region in Africa reported that literacy, language, possession of identity cards and poverty are among barriers to use of mobile money services [28].

The importance of assessing human *capabilities* in contexts has been discussed by Joinson and Steen [29] without enumerating what they are. The notion and intent of opportunities there ties in with the concept of freedom which lies at the core of the *capability approach*. Individuals want to help themselves and influence the world [30]; this means individuals are active agents with their own doings and beings. A digital space which intends to be inclusive accommodates diverse individuals with their doings and beings [4]. To that end, Marx's principle of *the development of each as a condition of development for all* is recommended as the guiding principle by Toews [31] to bridge the digital divide. The authors explicitly argue for everyone to have a fair share of access to the digital space in a manner they *value*. The realisation of which begins with evolving a list of *basic capabilities* for diverse groups in their contexts. Diversity of dispositions includes individuals with disability. A recent judgement involving capability and social media; a judge observed that disabled individuals should be able to use privacy controls [32].

Ani *et al.* [33] argues for knowledge as the foundation of other *capabilities*. This, we feel, needs a broadening of other focal variables such as age, gender, and ability, among other things, to appropriately assess the role knowledge can play. There are also discussions around *capabilities* in organised settings [34]. Our interest in aggregate capabilities are to make a inter-personal comparison of welfare (capabilities, freedom).

3.1.2 Security & Privacy Capabilities:

Luo *et al.* [35] interviewed public library IT staff to understand the challenges faced them in implementing security & privacy policies. The authors frame their findings using Sen's *capability approach*. The study conveys significant insights on *capabilities* that library staff should have; for example, protecting their patrons from surveillance. Such insights can be built upon to make the barriers faced by library IT staff as focal variables of provisioning efforts by the security & privacy community.

Riley [36] points out that online health networks, while enabling sharing of health-related information, also pose serious risks to individual privacy. The General Data Protection Regulation (GDPR) codifies individual rights to privacy and include significant rights such as *right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object* and the *right not to be subject to a decision based solely on automated processing*. These are important rights, but places disproportionate load on individuals [37]. Such rights need to revolve around a nuanced assessment of individual opportunities to use them [38]. Perera *et al.* [39] highlights the lack of resources to transform GDPR principles reflecting power, security and universalism into actionable guidelines software developers can use. A recognition of the fact that application developers do not have the opportunities to implement them can lead to policy debates about provisioning the basic minimum for them to implement those guidelines effectively.

A survey-based study [40] recognises the awareness of healthcare staff in observing cybersecurity hygiene and proposes awareness training, nudges and champions. Their survey did not consider individual lived experiences and other dispositions which can lead to a comprehensive assessment of the opportunities individuals working in healthcare have to observe cybersecurity hygiene and/or make effective use of the interventions intended to help them. The importance of capturing factors such as culture, lived experiences beyond human interface with technologies is also argued by Rohan *et al.* [41].

3.2 Q2: Proposed Solutions

Prior research looked at human physical *capabilities* to prevent cyber attacks. Oltramari *et al.* [42] argues for assessing knowledge, skills and overall risk assessment capabilities for a holistic assessment of risk in an organisational context. A proposed framework to enhance the resilience of employees in small and medium enterprises depends on *capabilities* to anticipate, monitor, respond and learn [43]. Some studies argue that better interfaces improve the capability of humans to detect phishing emails [44]. This does not consider the needs and diversities of the users themselves. Their *functionings* in their situations would not reliably benefit from interface refinements. Similarly, tools to detect the ability of cybersecurity professionals to respond to Intrusion Detection System (IDS) alerts are built on the presumption of antecedent uniformity [45].

Mehrnezhad *et al.* [46] argue that most CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart) [47] rely on human visual recognition abilities. They suggest the deployment of CAPTCHAs that rely on: (1) ability to recognise an image's orientation, (2) the human brain's ability to guess the whole artefact based on partial presentation, and (3) decision making when challenged by a puzzle. Their work unrealistically assumes adequate vision and unimpaired cognition [48]. The expectations of adequate eye-sight and unimpaired cognition are relevant findings in the assessment of opportunities diverse individuals have to pass a CAPTCHA test.

Some interventions assess the abilities of individuals through various data points such as their qualification *vis-a-vis* the systems they are supposed to operate [49]. Yet, such assessment of abilities tend to be information poor. Formal education is one of the many data points required to make an adequate assessment of human diversity. Others suggest improvement in mental models and cognition [50]. From a *capability approach* point of view, such interventions cannot stand without an adequate understanding of the target population they aim to empower.

Capability approach is interested in the physical abilities, education and ability to respond to risks, to the extent that they are adequately considered to lay down *capabilities* to achieve certain *functionings* and not to exclude individuals without a prescribed physical ability or with diverse cognitive skills.

3.3 Q3: Criticisms

While we explored the application of the *capability approach* in the use and protection of ICTs, we found literature that points to its shortcomings. Stella and Corry [51] point to the vagueness of the *capability approach*. Gasper [52] highlights difficulties in operationalising the capability approach also citing its vagueness. Gasper argues for a maturation to take place to ensure that the approach delivers on its potential. They also argue that *capability approach* does not articulate the causes of inequality which is an impediment to its application.

3.4 Implications for our Study

3.4.1 Summary of Findings.

This discussion of capabilities-related research demonstrated that the cybersecurity and privacy literature has only intermittently engaged with the foundational concepts and expositions of the *capability approach*. We acknowledge the criticisms of the capability approach, but argue that this very vagueness can actually be a strength rather than a weakness. Sen steered clear of giving it an epistemological status as "the capability approach" and left it as a framework of thought [24]. Moreover, its abstract nature allows inequalities and their reasons to surface empirically, making it possible for responsible stakeholders to frame policies and interventions attuned to individual needs. To encourage engagement, a contextual list of *basic capabilities* is needed to ground the approach.

3.4.2 Demographic to Target.

Capability approach, as a methodology, aims to capture the *needs* of individuals in their diversity. The individual is of moral concern to the extent that individual needs should not get subsumed under the collective identity of the group they belong to. It is infeasible to attempt to arrive at a full list of *basic capabilities (cybersecurity)* for all demographics in one fell swoop. We wanted to choose a demographic with three features: (1) large enough numbers to support an investigation, (2) having capability issues, and (3) being particularly vulnerable to cyber attacks. We thus decided to focus on the the over 65s, who satisfy all our requirements.

In the first place, there is a global increase in the 'graying population' [53] in high income countries (Figure 3), making them a significant part of the population. In the second place, this demographic commonly suffers from age-related infirmities and capability loss [9, 54–56] and have limited disposable income. They are also very likely to be targeted by cyber criminals [57]. A study of older adults with mild cognitive impairment in the United States revealed that almost all families had fallen victim to at least one minor security incident online [58]. A recent study [59] highlights that older adults are unaware of the threats due to usage of second hand devices, devices in public places and there is a feeling of resignation among them about privacy [59]. Elderly citizens feel they are excluded by system designers [60, 61].

Given the widespread digital push towards accessing health and welfare services online, there is a genuine need to accommodate the needs of senior citizens. Their minimum capacities or reasons to act align with the barriers they face and, as a result, many older adults can not participate in the online community [62, 63].

Hence, as a first attempt to arrive at a list of basic capabilities, we will aim to reveal a list of *basic capabilities (cybersecurity)* for

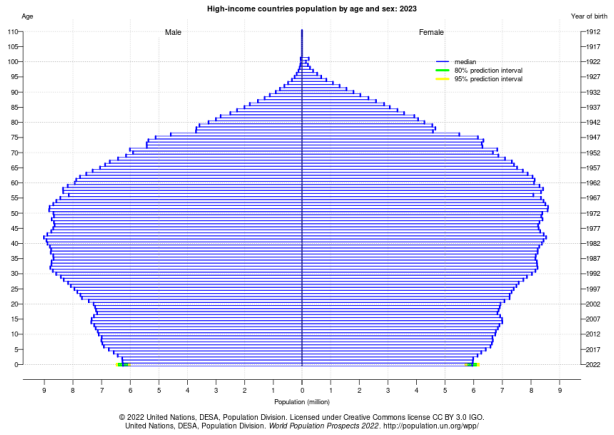

Figure 3: Population Profile for High Income Countries [65]

seniors carrying out core cybersecurity hygiene tasks. Our endeavour is a departure from narrow accessibility perspectives and rather provokes policy makers to mandate *basic capabilities (cybersecurity)* so that developers re-imagine protection mechanisms to suit the needs of older adults as well as others [58, 64].

4 BASIC CAPABILITIES (CYBERSECURITY)

4.1 Study Procedure:

We situate our understanding of the reasons for elderly citizens to act with respect to the barriers to perform the following cybersecurity hygiene tasks (see Table 1):

(1) Use Strong Passwords.
(2) Keep your software and systems fully up to date.
(3) Use Multifactor Authentication (MFA).
(4) Secure your Home WiFi.
(5) Back up your Data.

Note that due to the low adoption rates of password managers across the entire population [66], and the recency of the LastPass Password Manager breach[1], we do not include this particular advisory.

The idea is to use these tasks to elicit *basic capabilities (cybersecurity)*, the most compelling reason for individuals to act, or not to act [67]. Survey questions are provided in Appendix A. Respondents were asked to answer all questions in the survey. Bonuses were paid for comprehensive responses.

We asked three over 60s to pilot the survey and then checked Qualtrics for the amount of time it took. We asked them to give us feedback about the clarity of the questions— they did not report any issues that warranted a change in the scenario formulation. We discarded their responses and did not include their data in our analysis.

4.2 Recruitment & Ethics

Senior citizens living in the UK, the USA, South Africa, Botswana, Nigeria, Canada, India and Australia who were fluent in English

[1] https://blog.lastpass.com/2023/03/security-incident-update-recommended-actions/

	NCSC[1] UK	CISA[2] USA	Govt of Canada[3]
1. Use Strong Passwords	✔	✔	✔
2. Keep your software and systems fully up to date	✔	✔	✔
3. Use Multifactor Authentication	✔	✔	✔
4. Secure your Home WiFi			✔
5. Back up your Data	✔		✔
[1]National Cybersecurity Centre (NCSC) (UK): https://www.ncsc.gov.uk/section/information-for/individuals-families			
[2]Cybersecurity & Infrastructure Agency (CISA) (USA): https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe			
[3]Canadian Government: https://www.cyber.gc.ca/en/guidance/cyber-hygiene			

Table 1: Government Cyber Advisories

and 65 years of age or older were recruited from the Prolific platform to participate. We chose this range of countries to maximise geographic diversity. Prolific makes it possible to balance gender of respondents, and also to request specific age ranges. We did not collect demographic data, in accordance with the rules of the platform. Participants were paid the UK living wage, and given a bonus for comprehensive answers. Ethical approval was obtained from the University of Strathclyde and the REPHRAIN Ethics Review Board.

4.3 Adherence to SIGSOFT guidelines:

The adherence of various aspects of the study to [68] can be summarised as:

- We recruited participants adhering to the relevant *essential attributes* of [68].
- The answers were free flowing text. They were analysed one participant at a time as outlined in *application* of [68].
- In Section 4.4, we outline how we achieved saturation. This is in line with the *essential attributes* [68].
- We present the findings of our study as per all the relevant *essential attributes* and some of the *desirable attributes* of [68].
- The survey text did not prompt the respondents to avoid any bias. This is in line with the relevant guideline under *essential attributes* of [68].

4.4 Analysis

We used a collaborative platform Miro [69] to support analysis of the data. Our analysis followed Braun and Clarke's [70] staged thematic analysis approach. We commenced with data familiarisation, then continued to initial code generation, thematic search and finally agreed on final themes. The researchers independently and systematically coded the responses. Longer sentences were coded into smaller phrases or words. A statement such as "*if her eyesight is failing it might be difficult*" (P1) was coded as *statements describing vision* as 1^{st} order code and subsequently into *accessibility issues* as 2^{nd} order theme.

4.5 Threats to Validity

Participants were recruited from the Prolific platform. This means, on the one hand, that they are accustomed to working with technology, and probably better informed than the average retiree. On the other hand, this also puts them in a good position to be aware of potential barriers and challenges faced by people of their age.

The survey study allowed individuals to respond with free text. This was to encourage them to provide comprehensive responses. However, face to face conversations can elicit more information and provide the opportunity to ask follow-up questions.

While we adhered to the criterion of context in choosing our participants, this can be further refined in terms of gender and other conditions. That can potentially elicit more nuanced understanding of needs. *Capability approach*, being a framework of thought, inherently allows such granularity. Thus, this study while is a significant first step, can be further granulated.

There is a possibility that our results are more applicable to elderly citizens who are more active online compared to those who are not. However age related infirmities can be found even in those who are less active online.

The list of *basic capabilities (cybersecurity)* we present as an output of this work needs to be validated for technical and political feasibility. We treat this as a 'work in progress', which will be refined through further research in this area.

5 BASIC CAPABILITIES (CYBERSECURITY) FOR SENIORS

We present the results of our survey study here. Each subsection sums up the barriers (as described by the participants) particular to a task. Task specific list of *basic capabilities* is presented at the end of each subsection to set them in context. Figure 4's Column A presents 1^{st} order codes for *all* tasks while Column B reflects *task-specific* 1^{st} order codes. (The tasks are indicated in brackets next to the codes in Column B.) Column C shows the 2^{nd} order themes that emerged from 1^{st} order themes mentioned in Columns A & B.

We will discuss the 2^{nd} order themes in the context of specific cybersecurity hygiene tasks. *Skills, emotions. social aspects and externalities* were common across all of the task scenarios we presented to the participants. *Accessibility issues* emerged in four of the cybersecurity hygiene tasks. *Time pressure, trust, clarity and human bias* were specific to certain tasks. Representative quotes for each of the 2^{nd} order themes are provided in Figure 5. The representation is inspired by similar work on barriers in the domain of healthcare [71], though our themes are different.

5.1 Methodology

The *basic capabilities (cybersecurity)* we present below are illustrative and not a comprehensive list of indispositions. They can act as a foundation upon which future research can build to develop a more nuanced evaluation of capability inequalities amongst the elderly

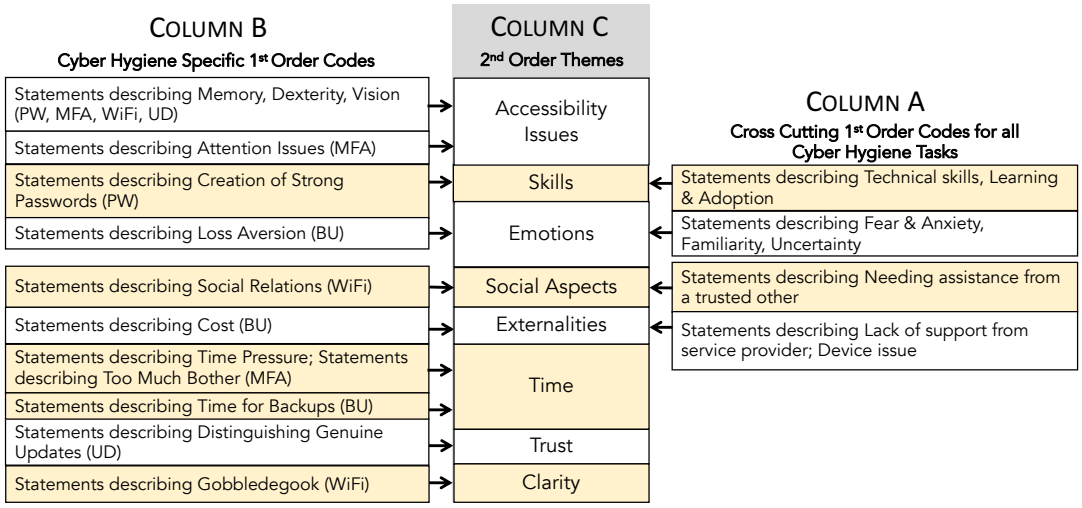

Figure 4: Column C are the top-level themes with column A reflecting the cross-cutting 1st order codes and column B indicating 1st order codes specific to particular tasks (indicated in brackets next to the code in column B). (PW=strong passwords, UP=make updates, BU=make backups, MFA=Multifactor Authentication)

population. This can help to inform design of equitable provisioning of mechanisms pertaining to cybersecurity hygiene tasks.

The list should be ***methodologically justified***. While doing this research, we commenced by engaging with relevant literature on *capabilities*. This was carried out in order to draft a candidate list by engaging with existing academic and grassroots literature. There is a gap in systematic implementation of *capability approach* in prior research. Subsequently, we followed Sen's method of evolving a contextual list. We focused our efforts on elderly citizens and their context and adhered to the established criterion for generating such a list as enumerated in Section 4.2. Our list of *basic capabilities (cybersecurity)* is grounded in the criterion as follows:

Criterion of Explicit Formulation urges us to go beyond what is reflected through democratic choice. While we analyzed the data we did not constrain ourselves in numbers to elicit what is said by majority of our participants. The authors engaged in unconstrained deliberation to bring out individual indispositions. This is in line with the fundamental ethos of *capability approach* where the individual is of primary moral concern.

Criterion of Sensitivity to Context led us to choose a particular section of the population for whom age related indispositions are a reality. The focus of our study was eliciting their needs based on the opportunities they have. This elicits issues related to memory, vision, arthritic fingers and mobility among others. Mechanisms that are cognisant of such semi-permanent conditions that they might have to live with for the rest of their lives are their basic need and will determine if they would choose to act with respect to the 5 cybersecurity hygiene tasks. So our list of *basic capabilities (cybersecurity)* speaks the language of those they are meant to protect.

Criterion of Different Levels of Generality specifies a unconstrained list which can be refined to a subset that can be implemented in the near future given the political, social and technical realities of the day. The list of *basic capabilities (cybersecurity)* we propose pertaining to each of the tasks are akin to an ideal list. The reason being they are yet to be assessed for their feasibility. They might need further refinement and one future work we do consider is to speak to system developers and experts on the feasibility of our list. Nevertheless, our list makes a strong case for changing the technical and political realities.

Criterion of Exhaustion & Non-Reduction: In our list of *basic capabilities (cybersecurity)*, we include every barrier identified by our participants to be considered as a focal variable. The *basic capabilities* that evolved are distinct with negligible overlaps.

5.2 Barriers to Creating Strong Passwords

We presented our participants with a scenario where Bob, a senior citizen in his 80s, needs to update the password he uses to access his online banking service.

Accessibility issues emerge due to concerns of participants with respect to memory, vision, dexterity so on and so forth. "*Choosing a password that is unique and hard to hack but could also cause him future problems in remembering it without writing it down*" (P33).

Skills with respect to passwords include the ability frame secure passwords — "*Bob might have difficulty coming up with a new password that meets the bank's requirements (e.g., number of characters, combination of letters, numerals and special characters) and then he might have trouble remembering the password*" (P15).

Emotions figure prominently as a barrier in the responses of our participants with respect to framing secure passwords.

> *"The first problem is that some banks do not tell you what a password must consist of, so he may waste a lot of time thinking up a password only to have it rejected and only then get a message saying 'passwords must contain.....' If Bob has attention span problems, high blood pressure or agitation then he may not be able to complete the task"* (P51).

ACCESSIBILITY	EXTERNALITIES	TIME	CLARITY
"might have vision problems so she may find it difficult to see the code on her phone" (P14)	"my mobile is only a cheap standard type" (P48) "cost too much" (P53)	"be able to clearly see the code sent in a text message and only has a limited time to enter it" (P63)	"unable to understand the instructions, she might also have trouble remembering her password" (P20)
HUMAN BIAS	**SKILLS**		**SOCIAL ASPECTS**
"he would most certainly not want to lose these precious memories" (P58)	"understanding the terminology could very well be an issue" (P23) "might have difficulty understanding the technical aspects she needs to take. She may lack confidence in her ability to carry to the necessary actions" (P59)		"best policy is to request help, either from a friend, or possibly a local shop" (P17)
TRUST		**EMOTIONAL STATE**	
"he might find it difficult to establish if the update is genuine or some sort of scam" (P12) "she will want to be very wary of the source of the info that she is getting" (P62)		"she may also be anxious about the situation" (P54) "can only have negative consequences for him" (P62) "there may be some embarrassment that she has not protected her network with a password" (P52)	

Figure 5: Quotes for each 2nd Order Theme (using barrier headings from [71])

Social aspects highlight the importance of the availability of help from family and friends — "*Youngsters seem to naturally adapt to new tech so does Bob have any children? he could ask them - not for an actual password, but guidelines*" (P53).

Externality for passwords outlines the difficulties due to device failure and the consequent recovery — "*he might have the devil of a job retrieving it in the event of a computer failure. (And the auto-generated passwords are largely incomprehensible!)*" (P43).

There are lab based user studies with respect to password creation. A notable study conducted with 49 participants situated around a university campus reveal their strategies with respect to password creation [72]. While the study brings important insights with respect to propensity to reuse passwords mental models and perceptions of end users, there remains a need to study individual indispositions. While we investigate the needs of the elderly the constraints e.g. living alone comes across as an important blocker. Such barriers inform the *basic capabilities (cybersecurity)* elderly individuals living alone must have to be able to formulate secure passwords.

Basic Capabilities (Cybersecurity) for inclusive access control using secure passwords provisioning:

- Ability to manage secure passwords unimpaired by:
  (1) attention difficulties,
  (2) hypertension,
  (3) cognitive impairments,
  (4) anxiety,
  (5) memory issues,
  (6) slow or arthritic hands (dexterity limitations),
  (7) vision impairments.
- Ability to recover if passwords are forgotten.
- Ability to use passwords without fear of being excluded.

5.3 Barriers to Regular Updates

Our example scenario was about an 80 year old retiree, John. He is required to process an update request on his phone.

Accessibility Issues were highlighted by our participants due to vision or age induced physical impairments.

> *"John might not know how to navigate the menus to get to the update page and if he does find it he may get a bit confused about what he might have to do next. Also if has vision difficulties or arthritis then the above problems would be more severe"* (P14).

The quote is also representative of the difficulty in technically navigating the update process.

Skills emerge a concern for applying updates similar to other tasks. "*He may not know how to access the settings app and then download the new update*" (P28). "*John would need to understand what is an update and why he needs to update. The second challenge is to learn how to update his phone*" (P38).

Emotions in the context of applying updates highlight the sense of anxiety, shame, fear that elderly citizens might feel in seeking help. "*He may worry that he would look silly in asking for help*" (P42). There is also associated anxiety and fear that elderly citizens feel with respect to having to update a new phone. "*Thirdly he would be anxious because it is a brand new phone and people our age don't expect things to need updating immediately you buy it*" (P51).

Social aspects emerge in case of updates with respect to the ability to seek assistance from close family and friends. "*If in doubt ,ask a trusted family member or friend. "* (P17)"*My mother asks me to install updates as she thinks she is being scammed*" (P13).

Externalities refer to the availability of help to process and apply the updates. Elderly citizens who are more attuned to physical communications might want to access help if there are glitches during the update process. "*The software update could have a glitch in the update so he should know what to do*" (P11).

Trust emerges as a specific theme in case of updates from our data. Participants highlight the need to discern phishing messages from

genuine updates. "*I wouldn't update software just from a message on his phone, scams are everywhere, as its a brand new smartphone why does it need updating*" (P20).

A notable study investigates the usage of libraries by developers and their requirements of updates [73]. While versioning, better communication contribute to increase in propagation of updates, there is a need for considering user groups in their situations like age. *Basic capabilities (cybersecurity)* formalises mechanisms that help individuals with issues such as their age related vision, as minimum necessary conditions for them to be able to update their applications.

Basic Capabilities (Cybersecurity) for inclusive update propagation mechanisms provisioning:

- Ability to navigate application update menus unimpaired by:
  (1) vision impairments,
  (2) dexterity limitations.
- Sufficient education to understand why to update.
- Ability to discern a genuine from a malicious update.
- Ability to obtain assistance during the update process.
- Ability to cope with the unfamiliarity of updated device/application.

5.4 Barriers to Multifactor Authentication (MFA)

The scenario described a senior citizen, Sadie, who uses her phone and computer to stay connected with her family. She is new to online banking and the bank requires her to set up multifactor authentication (MFA).

Accessibility issues were highlighted by participants and they include the ability to remember the process, the code, eyesight, mobility, time constraint and memory issues.

> *"Sadie may face challenges in remembering the two factor authentication method. If her phone is not in front of her and she has to walk a distance to get it then if she has mobility issues she may not be able to get to her phone quick enough, as the code is only valid for a certain amount of minutes"* (P49).

Skills figure among the overwhelming concerns expressed by the participants. This indicates that elderly users might not be technically equipped and learning new skills at an advanced age can burden them. "*Sadie might not understand the process and may not be cognizant with the smartphone (she may use for communication only)*" (P13).

Emotions emerged as a 2^{nd} order theme as participants highlighted *fear, anxiety, uncertainty and familiarity* as part of this adoption. "*If she has trembles, anxiety, hypertension, short attention span, etc then she is at a grave disadvantage having to use 2 factor log in*" (P51).

Attention span emerges as a 1^{st} order code with respect to MFA in our analysis.

Social aspects of carrying out the particular task was highlighted by our participants. "*She may need to get help from a trusted friend or relative to help her when she wants to do online banking on her phone*" (P57).

Externalities like access to a network and appropriate device were highlighted in the context of MFA. "*I have a friend (f,75) who has to walk 100 metres up her drive to get a signal - and of course the page has timed out by the time she gets back*" (P19). This also relates to our 2^{nd} order theme **time pressure**, which impairs individuals with other indispositions apart from poor network. There are individuals with slow fingers, or age-induced immobility. "*Having two windows open at the same time can be awkward. It can be difficult to memorise a code and it can disappear before it can be written down*" (P22).

Time emerged as a 2^{nd} order theme with respect to MFA. Though we enumerate quotes expressing the influence of time pressure on other themes, yet the overwhelming concern expressed by our participants led us to situate this as an independent theme.

> *"Being able to see the code and enter it into her account without being timed out. If she has used her computer and smartphone for a long time she would not find this too difficult to do. Giving her enough time to enter would be the most challenging thing"* (P42).

There are prior studies with respect to usability of MFA. Concerns around security and being locked out of their accounts were discussed in prior research [74], the study recruited participants between ages of 21-44 and fairly experienced with MFA. A related study [75] investigated the usability reasons behind the *limited diffusion* of MFA. Their findings highlight the usability challenges with the interface. While evaluation of interaction with surface features provides useful insights they are not meant to elicit variation in personal conditions like vision, slow fingers and make them focal considerations for MFA mechanism designers. For equitable ability to use MFA there needs to be supporting mechanisms; *basic capabilities (cybersecurity)* informs minimum focal considerations for system designers to achieve equitable provisioning.

Basic Capabilities (Cybersecurity) for inclusive MFA provisioning:

- Ability to adopt MFA unimpaired by hypertension or anxiety.
- Ability to manage MFA codes unimpaired by:
  (1) vision impairments,
  (2) memory issues,
  (3) attention difficulties,
  (4) time constraints,
  (5) network connectivity issues.
- Ability to use MFA without fear of being excluded.

5.5 Barriers to Securely Setting up WiFi

Karabo is a senior citizen in her mid 70s learnt that her neighbours are using her WiFi password. She needs to set a secure password for her WiFi.

Accessibility issues were flagged by participants as understanding the process would be difficult for elderly participants to understand the process and age related ailments might come in their way. "*Understanding the way to do it from her research and feeling confident doing. Also impaired eyesight might make this more difficult*" (P32). Similar to findings with setting up secure password (Section 5.2)

participants flagged the need to set up a strong yet easy to remember password — "*The main issues are to choose something that the neighbours are unlikely to be able to guess (so not her own name or that of the dog) and to remember the new password!*" (P50)

Skills was flagged by participants in terms of elderly persons being able to do the configuration by themselves and find the reason for the breach. "*Would Karabo be able to complete the process? It may be a long and complicated process.*" (P49) "*Another difficulty facing Karabo is understanding how the situation has occurred in the first place*" (P47).

Participants highlighted situations which overlaps between **accessibility issues** and *skills*. "*You may have reduced mobility in you hands making it difficult to navigate the menus, also it is harder for old people to learn new stuff*" (P62).

Emotions emerged as a second order theme in case of setting up WiFi password due to the failure to keep the network secure. "*There may be some embarrassment that she has not protected her network with a password, which could stop her asking family or friends to set one up for her*" (P52). Participants also related to the anxiety faced by a victim whose network security is compromised — "*She may also be anxious about the situation*" (P54).

Social aspects was highlighted by our participants due to need to seek assistance and a potential the eventuality where the victim might need to confront their neighbors. "*I would hope she might be able to seek advice from competent friends about the situation*" (P43). Participants also highlighted the possibility of aggravated situations —" *It would be good if one of her family helped her to confront her neighbours on the matter*" (P45). Participants suggested seeking help from close family. Participants highlighted the conflict scenario along with *fear* where by mal-actors could cause her harm, breach her privacy or push malware into the network.

Externalities manifest in the form lack of adequate support from service providers. Participants shared their own experiences of their interaction with their service providers — "*It looks like she is quite clued up, but she might not know how to get an effective response from her service provider, because most of them try hard to avoid customer questions, ours certainly does*" (P53).

Clarity of the advice shared by service providers were also flagged by participants both in terms of language as well as usable communication. "*Possible challenges ... is English her first language? If not then understanding instructions could be a challenge*" (P56).

Prior research explored users' ability to configure home WiFi. A user study evaluated the ability of 30 participants without any formal training to set up low-cost WiFi devices. They report the usability advantages of some of the devices over others [76]. The findings pertaining to non-technical users' ability to interface with limited menu options are useful but fall short of bringing out their needs in their situations. For example, impaired eye sight is a barrier in securely setting up secure WiFi and can further exacerbate the difficulties that result out of limited menu options. Inclusive systems engineering needs to be privileged on an understanding of such inequalities. Formulation of *basic capabilities (cybersecurity)* upon individual needs is ideally placed to drive the policy and provisioning conversations of systems engineering.

Basic Capabilities (Cybersecurity) for inclusive secure WiFi configuration mechanisms provisioning:

- Ability to set up secure WiFi, unimpaired by:
  (1) vision impairments,
  (2) memory issues,
  (3) cognitive impairments,
  (4) low literacy,
  (5) dexterity limitations.
- Ability to get assistance from router manufacturers.

5.6 Barriers to Making Backups

Our participants were presented with a scenario where 65 year old Lindiwe likes to take pictures of her family and friends. She would like to back up those precious memories.

Skills were highlighted by participants of our study as a barrier in the context of elderly users. "*When not having been taught anything at all about modern day technology, it is time consuming researching how to do it oneself*" (P36). "*Lindiwe could encounter difficulties backing up her photographs, depending on the type of media she decides to use*" (P27). Participants also expressed their frustration about the process —"*A simple operation? Stalled at '95 referenced files in your library will not upload to iCloud Photos.' and then having to go on a Google hunt to find out what [redacted] that meant*" (P43).

Emotions in terms of fear and anxiety over losing precious memories were highlighted by our participants. "*She could also delete her photos accidentally if she did something wrong.*" (P29) There can concerns among the elderly about their pictures getting exposed to unauthorised entities — "*She may also worry if these photos could be used by other people without her knowledge*" (P56).

Social aspects came up as a theme with respect to back ups due responses seeking help from close family and friends. While there are participants who has family relations to take help from — "*I think my daughter uses a little thingy! that she downloads them on to*" (P20). On a general note, participants suggested seeking help from friends and family. "*She might have trouble understanding what to do, it becomes more difficult to understand the technology as you get older and you need help from a younger member of the family. She might not understand the cloud*" (P21). An absence of the ability to seek help constitute as a barrier.

Externality in case of back ups, these manifest as an ability to access use an external service providers. Such an ability can be perturbed by lack of transparency and available help. *Cost* came as hidden factor from our participants. "*Choosing the right platform for backing up photos is difficult. Many can be expensive - some have extra charges hidden in the small print when you sign up*" (P26).

Time is highlighted in the context of back-ups. Participants highlight that backing up images need time and users should have the patience to let the process complete. "*Also has to realise that it can take a long time to back everything up*" (P25).

There are usability studies of Google products like Google Plus, Drive with students [77]. The study reported that Plus has marginally more usability advantages over Drive and Google Classroom environment had significantly more usability advantages over others. While these are important insights they need to expand beyond evaluation of surface features to an understanding of needs. Situating

basic capabilities (cybersecurity) drives the provisioning of comprehensive mechanisms, to support individuals with conditions such as age related learning impairment, as basic minimum in the adoption of cloud back ups.

Basic Capabilities (Cybersecurity) for inclusive back up configuration mechanisms provisioning:

- Ability to identify a trustworthy back up service provider.
- Ability to make backups without:
  (1) accidentally deleting files,
  (2) insufficient understanding of backup technology,
  (3) lack of means to pay for a backup service,
  (4) fear of losing privacy.
- Ability to use backups to recover files.

6 AGENDA FOR FUTURE RESEARCH

Inclusive provisioning of secure Internet requires a clear understanding of the nature of poverty suffered by the very individuals. Measuring security and privacy poverty is a timely need and we outline a research agenda based on the *basic capabilities* proposed in Table 2. Engineering *basic capabilities* involve appropriate comprehension of the concepts by system engineers, pertinent threat modelling, security communication and aiding developers to achieve all that. We outline a research agenda as:

6.1 Security & Privacy Poverty Assessment

Poverty is absence of basic minimum capabilities [78]. Individuals without the opportunity to achieve some minimally acceptable level of functionings are classified to be living in poverty. For example, the ability to live, to be fed and clothed enable individuals to unlock other significant functionings. Individuals who are not adequately clothed or fed or do not have access to healthcare live in abject poverty and there are various measures of poverty like household income and means of sustainable living [79].

It is important to deliberate on the criterion to measure poverty. Should the consideration be on one reason or plural indispositions? A person can have income but is disabled to access healthcare. In that case stipulating income as a sole measure leaves the disabled person out of provisioning policy for healthcare. Situating absence of *basic capabilities* as a measure of poverty recognizes that there can be multiple reasons behind their poverty. A list of *basic capabilities* moves beyond a singular factor to measure poverty, rather focuses on all the focal variables that enables citizens to live a minimally adequate life.

Including elderly citizens in a digital first society would require a foundational understanding of their security and privacy poverty *i.e.* the nature and scale of the problem we intend to address. The pertinent question for us is how we should go about measuring security and privacy poverty. Adequate measurement is key to eradication, and should also apply to security and privacy poverty [80].

We draw from the formulation of poverty as absence of one or many *basic capabilities* [78] for measuring security & privacy poverty . Our results in Section 5 point to the fact that there are various reasons behind the lack of opportunity for elderly persons to perform those cybersecurity hygiene tasks. For example someone can have good eye sight but arthritic hands or poor network connectivity to use MFA. Some can have all the indispositions. Table 2 is a candidate list of the minimum basic capabilities that elderly citizens need to adopt the cybersecurity hygiene activities recommended by governments. They speak of various abilities which together can enable a particular functioning. For example, a functioning like MFA requires capability to do so with arthritic hands, poor vision and access to a Smart phone in most cases. Absence of these *basic capabilities (cybersecurity)* means individuals are poor in achieving a particular functioning. Absence of one for some or absence of all for others would mean such individuals are in poor in achieving this functioning. The measurement should be on absence of multiple factors rather than one in any list of *basic capabilities (cybersecurity)* in any context.

Our work can serve as a useful foundation to assess security and privacy poverty and subsequent eradication. *Basic capabilities (cybersecurity)* give individuals the freedom to choose from available functionings in a manner compatible with their dignity. Furthermore, we evolve them through empirical data. Our methodology recognises humans as active agents with their own *beings* and *doings*. Consequently, the *basic capabilities (cybersecurity)* list is inherently and adequately influenced by variations in personal and social circumstances. This plurality of (in)dispositions is significant for comprehensive security and privacy poverty eradication and can allow individuals to safely and securely participate in a 'digital first' society in a manner they *value*.

Agenda. Poverty removal is key to including disadvantaged groups in any welfare process. The danger lies in constraining the criterion used to measure poverty. That leaves out many who do not conform to the criterion. *Basic capabilities (cybersecurity)* help to address the limitation because these are grounded in a systematic understanding of diverse needs. Future research can employ this method to assess security and privacy poverty based on their needs rather than focusing only on maximising usability.

6.2 Engineering *Basic Capabilities (Cybersecurity)*

The list we present in this paper is a formative one and requires further assessment with application developers on its technical feasibility. They include among others, a reasonable understanding of *capabilities* in the context of *capability approach* to resolve any conflict of terminology, appropriate threat scoping with respect to new capabilities and addressing the challenges application developers can face to implement *basic capabilities*.

Our understanding of *capabilities* is distinct than the way it has been dealt in the context of systems engineering particularly operating systems. The notion of *capability* in operating systems has been associated with permissions where by they grant access to system artefacts [81, 82]. Resources come with labels or capabilities associated with them and the capability is protected by the hardware. Research into capabilities looked into optimizing kernel overhead [83]. Recent initiatives like CHERI allows propagation and revocation of *capabilities* among protected artefacts [84]. *Capabilities* in the context of *capability approach* means the freedom to achieve some functioning. This is in a positive sense, at a higher

Table 2: Basic Capabilities (Cybersecurity) required to carry out task.

Basic Capabilities *The ability to:*	**MFA**	**PW**	**SW**	**UD**	**BU**
INDIVIDUAL ABILITIES					
see well enough to do [task]	✔	✔	✔	✔	
do [task] with the required attention	✔	✔			
adopt [task] with the dexterity and mobility	✔	✔	✔	✔	
do [task] with required short- and long-term memory	✔	✔	✔		
frame secure passwords		✔			
read manufacturer's documents			✔		
recover from failure during execution of [task]		✔		✔	
EXTERNALITIES					
access sufficient funds to achieve [task]					✔
find and read usable [task] guidelines			✔		
discern a genuine from a malicious update				✔	
understand why to update				✔	
do [task] with necessary network connectivity	✔				
access assistance if needed			✔	✔	✔
identify a trustworthy service provider					✔
do [task] without time constraints	✔				✔
INDIVIDUAL EMOTIONS					
do [task] without embarrassment			✔		
do [task] without fear of being excluded	✔	✔			
do [task] without fear of loss of data					✔
do [task] without fear of loss of privacy					✔

MFA=Multifactor Authentication; PW=Strong Passwords; SW=Secure WiFi; UD=Make Updates; BU=Make Backups

level of abstraction and distinct to the goal of controlling access as in the context of operating system *capabilities*. There can be deliberations in the context system design as to the positive *capabilities* that systems at various level of abstraction need to have to support the list of *basic capabilities*.

While drawing up *basic capabilities (cybersecurity)* and provisioning them, lack of appropriate threat scoping might expose the very individuals for whom they are provisioned to previously unscoped threats. To support this argument we can draw from the provisions of desktop clients of end to end encrypted (E2EE) messaging applications. The messaging applications were initially designed for mobile phones and their desktop clients were added later. Perhaps usability was kept in the mind and to facilitate the same non malicious synchronization between mobile and desktop devices were allowed by the system designers. That exposed users of desktop clients to various threats [85]. Particularly in the context of victims of intimate partner violence or users of managed devices [86]. This means that with the evolution of features to existing security mechanisms like MFA to enable wider participation of disadvantaged groups needs to be accompanied by appropriate scoping of emergent threats.

We find in our results that communication of threats and breaches are important particularly for disadvantaged groups, should be done in a manner they can understand. Language is highlighted by our participants along with other deprivations like eye-sight, memory and other inequalities in their (in)dispositions. This can be further expanded by looking at mechanisms that are available to such users to recover from breaches. Communication of breaches and their subsequent recovery can be looked from the wider prism of *security audit functions* [87]. A scrutiny of the E2EE mechanisms reveal that some of them expect the user to detect and recover from breaches while some others leave the user out of the loop to detect such breaches and recover from them [86]. There needs to be mechanisms to communicate threats, breaches and recovery in a manner appropriate to the deprivations of the individuals they are meant to protect.

Future research needs to explore the extent to which application developers have the opportunities to implement *basic capabilities (cybersecurity)* in order to enable their users to achieve a basic minimum level of functioning. This is crucial to wide spread provisioning of protection mechanisms similar to other public goods. The field of Developer-Centered Security (DCS) investigates the challenges application developers face with respect to implementing their security tasks [88]. We draw from some of the studies in the field to highlight issues of comprehension with respect to implementing security and privacy.

There are challenges that application developers face navigating the health information access control structure landscape [89]. Privacy permissions is a related and pertinent issue applications find difficult to navigate. For them it is often difficult to ascertain the scope of permissions or they often seek unnecessary permissions due to the requirements of the libraries they use in their application [90]. The security library eco system suffers from misplaced assumptions about the skills, abilities and incentive of application developer, in turn negatively affecting their effective integration into applications [91]. The usage of online information sources are negatively affected by bias, false sense of security and their information needs to be adopted with care and caution [92, 93]. Our results show that users are concerned with interference to their familiarity while updating applications. This is also a barrier faced by application developers as propagating updates can interfere with the functionalities of their applications [73].

Agenda. Future research needs to focus on ways to equip application developers with adequate comprehension of *capability*, ground them with appropriate scoping of threats and investigate security audit functions commensurate with the deprivations of the very individuals they intend to protect.

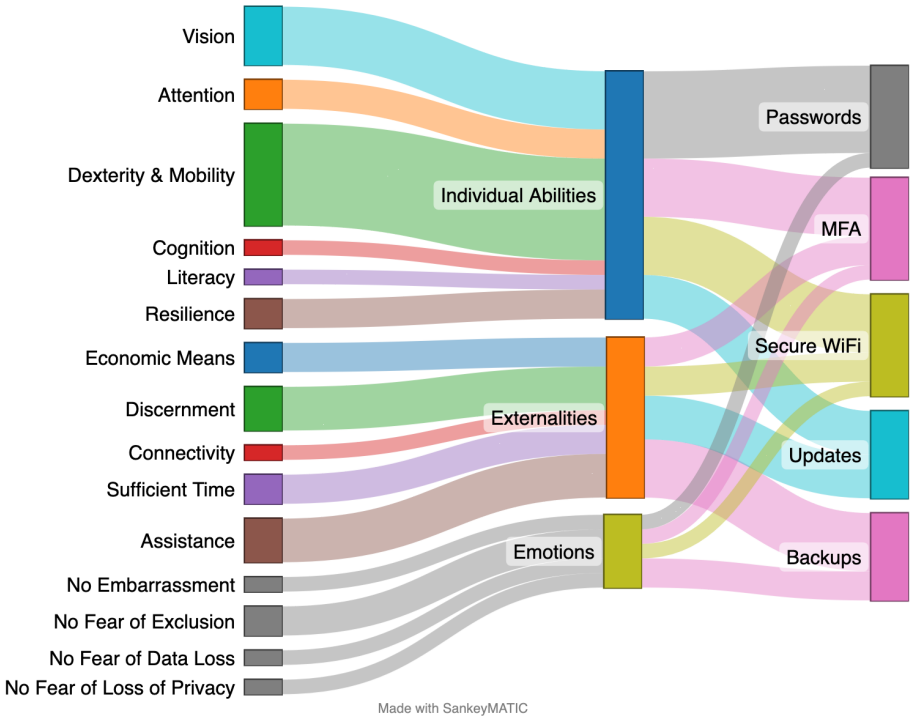

Figure 6: Final List of Cybersecurity Capabilities (Width reflects importance of Capability)

7 CONCLUSION

Prior research shows that digital systems are yet to meet the legitimate expectations of many marginalised groups [4, 94]. A 'digital first' society has unwittingly created a two-tier society where the fully capable enjoy secure participation while the less capable are left vulnerable. Securely participating in a 'digital first' society becomes difficult for individuals living under oppression, fleeing conflicts and those with other precarities such as age-induced infirmities [9].

Systemic exclusion has also been observed in provisioning of public goods in other spheres. This allows us to learn from other disciplines. The way democratic societies empower less privileged individuals to participate in areas such as finance, food security, and education is by making their needs focal variables of policy making and designing subsequent provisioning of public goods based on those focal variables [95].

This research endeavoured to reveal the needs and required cybersecurity capabilities of senior citizens through an understanding of the barriers they face in carrying out cybersecurity hygiene tasks. We see inhibiting factors such as impaired vision, failing memory, the need to rely on others to assist them, and less reliable cognition. This deters their ability to securely participate in the 21st century's 'digital first' society.

We use the findings to suggest a list of *basic capabilities (cybersecurity)* that makes individual indispositions focal variables of policy and subsequent implementation. The list needs to be further refined for technical and political feasibility. We discuss the engineering challenges such as conflicts in terminology with the way *capability* is being understood by the developer community. Our work can be seen as a foundation to formulate a comprehensive list to measure security and privacy poverty as the absence of capabilities to achieve basic minimum functioning. At the heart of our list is human diversity and the freedom to live a life people value. This is as much a moral need as is its criticality in maximising inclusivity.

ACKNOWLEDGMENTS

We thank the anonymous reviewers, Kopo Marvin Ramokapane and our shepherds Sara Correia and Ivan Flechais whose comments helped improve the paper greatly. This work is supported by REPHRAIN: National Research centre on Privacy, Harm Reduction and Adversarial Influence online (EPSRC Grant: EP/V011189/1). We gratefully acknowledge funding from the National Research Foundation of South Africa for this research. We acknowledge AP4L grant EP/W032473/1 for funding conference attendance.

REFERENCES

[1] P. Das Chowdhury, L. Coles-Kemp, K. Follis, S. Milivojevic, A. Rashid, G. Liveley, G. Netto, A. Dominguez, R. Anderson, and K. M. Ramokapane, "From utility to capability: A manifesto for equitable security and privacy for all," 2023, https://bpb-eu-w2.wpmucdn.com/blogs.bristol.ac.uk/dist/1/670/files/2023/02/Capability-Approach-Manifesto.pdf.

[2] L. Coles-Kemp and R. B. Jensen, "Accessing a new land: Designing for a social conceptualisation of access," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, ser. CHI '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 1–12, https://doi.org/10.1145/3290605.3300411.

[3] R. B. Jensen, L. Coles-Kemp, and R. Talhouk, *When the Civic Turn Turns Digital: Designing Safe and Secure Refugee Resettlement*. New York, NY, USA: Association for Computing Machinery, 2020, p. 1–14, https://doi.org/10.1145/3313831.3376245.

[4] N. McDonald and A. Forte, "The politics of privacy theories: Moving from norms to vulnerabilities," in *Proceedings of the CHI Conference on Human Factors in*

Computing Systems. Honolulu, USA, April 25 - 30: ACM, 2020, pp. 1–14, https://doi.org/10.1145/3313831.3376167.

[5] K. Renaud, G. Johnson, and J. Ophoff, "Dyslexia and password usage: accessibility in authentication design," in *Human Aspects of Information Security and Assurance: 14th IFIP WG 11.12 International Symposium, HAISA*. Mytilene, Lesbos, Greece, July 8–10: Springer, 2020, pp. 259–268, https://doi.org/10.1007/978-3-030-57404-8_20.

[6] K. Renaud and L. Coles-Kemp, "Accessible and inclusive cyber security: a nuanced and complex challenge," *SN Computer Science*, vol. 3, no. 5, pp. 1–14, 2022, https://doi.org/10.1007/s42979-022-01239-1.

[7] P. Das Chowdhury, A. D. Hernández, M. Ramokapane, and A. Rashid, "From Utility to Capability: A New Paradigm to Conceptualize and Develop Inclusive PETs," in *New Security Paradigms Workshop*, vol. Forthcoming. New Hampshire, USA: Association for Computing Machinery (ACM), 2022, https://doi.org/10.1145/3584318.3584323.

[8] J. Bentham, "An introduction to the principles of morals and legislation (1789)," in *The collected works of Jeremy Bentham*, J. H. Burns and H. L. A. Hart, Eds. New York: Clarendon Press, 1970.

[9] N. Warford, T. Matthews, K. Yang, O. Akgul, S. Consolvo, P. G. Kelley, N. Malkin, M. L. Mazurek, M. Sleeper, and K. Thomas, "SOK: A framework for unifying at-risk user research," in *IEEE Symposium on Security and Privacy (SP)*. San Francisco, USA: IEEE, 2022, pp. 2344–2360, https://doi.org/10.1109/SP46214.2022.9833643.

[10] A. K. Sen, "Universal health care," *Harvard Public Health Review*, vol. 5, pp. 1–8, 2015, https://www.jstor.org/stable/48503117.

[11] ——, "Equality of what?" in *McMurrin S Tanner Lectures on Human Values*. Cambridge, UK: Cambridge: Cambridge University Press, 1987, 1979, vol. 1, reprinted in John Rawls and Charles Fried and Amartya Sen and Thomas C Schelling. Sterling M. McMurrin (Ed), Liberty, Equality and Law.

[12] ——, *The Standard of Living*, ser. Tanner Lectures in Human Values, G. Hawthorn, Ed. Cambridge: Cambridge University Press, 1976.

[13] W. H. Organization, "Infant mortality," 2020, https://www.who.int/data/gho/data/themes/topics/indicator-groups/indicator-group-details/GHO/infant-mortality.

[14] B. Chakraborty, S. Yousefzadeh, S. Darak, and H. Haisma, ""We struggle with the earth everyday": parents' perspectives on the capabilities for healthy child growth in haor region of Bangladesh," *BMC Public Health*, vol. 20, no. 1, pp. 1–14, 2020, https://doi.org/10.1186/s12889-020-8196-9.

[15] T. Lin, D. E. Capecci, D. M. Ellis, H. A. Rocha, S. Dommaraju, D. S. Oliveira, and N. C. Ebner, "Susceptibility to spear-phishing emails: Effects of internet user demographics and email content," *ACM Transactions on Computer-Human Interaction (TOCHI)*, vol. 26, no. 5, pp. 1–28, 2019, https://doi.org/10.1145/3336141.

[16] S. Baki and R. M. Verma, "Sixteen years of phishing user studies: What have we learned?" *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 2, pp. 1200–1212, 2022, 10.1109/TDSC.2022.3151103.

[17] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman, "Of passwords and people: measuring the effect of password-composition policies," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Vancouver, Canada: ACM, 2011, pp. 2595–2604, https://doi.org/10.1145/1978942.1979321.

[18] K. Renaud, R. Otondo, and M. Warkentin, ""This is the way 'I'create my passwords"... does the endowment effect deter people from changing the way they create their passwords?" *Computers & Security*, vol. 82, pp. 241–260, 2019, https://doi.org/10.1016/j.cose.2018.12.018.

[19] P. Das Chowdhury and B. Christianson, "More Security or Less Insecurity," in *The 18th International Security Protocols Workshop*, ser. Lecture Notes in Computer Science, B. Christianson and J. A. Malcolm, Eds., vol. 7061. Cambridge, UK: Springer Verlag, 2010, p. 115–119.

[20] A. Sen, "Rationality and social choice," *The American Economic Review*, vol. 85, no. 1, pp. 1–24, 1995.

[21] M. Sim, K. Hugenberg, T. Kohno, and F. Roesner, "A scalable inclusive security intervention to center marginalized & vulnerable populations in security & privacy design," in *New Security Paradigms Workshop*, 2023.

[22] T. Burchardt, "Capabilities and disability: the capabilities framework and the social model of disability," *Disability & Society*, vol. 19, no. 7, pp. 735–751, 2004, https://doi.org/10.1080/0968759042000284213.

[23] M. C. Nussbaum, "Women and human development: The capabilities approach," in *The Seeley Lectures*, ser. The Seeley Lectures. Cambridge, UK: Cambridge University Press, 2000, https://doi.org/10.1017/CBO9780511841286.

[24] A. K. Sen, "Capability and well-being," in *The Quality of Life*, M. Nussbaum and A. Sen, Eds. Oxford: Clarendon Press, 1993, pp. 9–29.

[25] H. Mitchell, "Information and communication technologies and the urban transformation of South African informal settlement communities," Master's thesis, Urban Planning and Management, University of Cape Town, 2014.

[26] P. Palvia, N. Baqir, and H. Nemati, "ICT for socio-economic development: A citizens' perspective," *Information & Management*, vol. 55, no. 2, pp. 160–176, 2018, https://doi.org/10.1016/j.im.2017.05.003.

[27] S. S. Mohammid, "Digital media, learning and social confidence: an ethnography of a small island knowledge society," Ph.D. dissertation, RMIT University, 2017.

[28] O. C. Otieno and S. Liyala, "Mobile money users' functionings and freedoms: Amartya Sen's capability approach," *World Journal of Computer Application and Technology*, vol. 6, no. 1, pp. 14–22, 2018, 10.13189/wjcat.2018.060102.

[29] A. Joinson and T. van Steen, "Human aspects of cyber security: Behaviour or culture change?" *Cyber Security: A Peer-Reviewed Journal*, vol. 1, no. 4, pp. 351–360, 2018.

[30] A. Sen, "The formulation of rational choice," *American Economic Review*, vol. 84, no. 2, pp. 385–90, 1994, https://www.jstor.org/stable/2117864.

[31] D. Toews, "A socially-just internet: The digital divide, cybercultural agency, and human capabilities," *Studies in Social Justice*, vol. 2, no. 1, pp. 67–78, 2008, https://doi.org/10.26522/ssj.v2i1.968.

[32] BAILLII, "England and Wales Court of Protection Decisions," 2019, https://www.bailii.org/ew/cases/EWCOP/2019/3.html.

[33] U. D. Ani, H. He, and A. Tiwari, "Human factor security: evaluating the cybersecurity capacity of the industrial workforce," *Journal of Systems and Information Technology*, vol. 21, no. 1, pp. 2–35, 2019, https://doi.org/10.1108/JSIT-02-2018-0028.

[34] P. Korherr and D. Kanbach, "Human-related capabilities in big data analytics: A taxonomy of human factors with impact on firm performance," *Review of Managerial Science*, vol. 17, p. 1943–1970, 2023, https://doi.org/10.1007/s11846-021-00506-4.

[35] A. F. Luo, N. Warford, S. Dooley, R. Greenstadt, M. L. Mazurek, and N. McDonald, "How Library IT Staff Navigate Privacy and Security Challenges and Responsibilities," *literacy*, vol. 36, no. 38, 2023.

[36] R. Taitingfong, C. S. Bloss, C. Triplett, J. Cakici, N. Garrison, S. Cole, J. A. Stoner, and L. Ohno-Machado, "A systematic literature review of Native American and Pacific Islanders' perspectives on health data privacy in the United States," *Journal of the American Medical Informatics Association*, vol. 27, no. 12, pp. 1987–1998, 10 2020, https://doi.org/10.1093/jamia/ocaa235.

[37] O. Ben-Shahar, "Data pollution," *Journal of Legal Analysis*, vol. 11, pp. 104–159, 2019.

[38] H. Habib, S. Pearman, J. Wang, Y. Zou, A. Acquisti, L. F. Cranor, N. Sadeh, and F. Schaub, ""it's a scavenger hunt": Usability of websites' opt-out and data deletion choices," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–12.

[39] H. Perera, W. Hussain, D. Mougouei, R. A. Shams, A. Nurwidyantoro, and J. Whittle, "Towards integrating human values into software: Mapping principles and rights of GDPR to values," in *27th international Requirements Engineering Conference (RE)*. Jeju, Korea (South): IEEE, 2019, pp. 404–409, https://doi.org/10.1109/RE.2019.00053.

[40] E. Argyridou, S. Nifakos, C. Laoudias, S. Panta, E. Panaousis, K. Chandramouli, D. Navarro-Llobet, J. Mora, P. P. Zamorano, and S. Bonacina, "Cyber hygiene methodology for raising cybersecurity and data privacy awareness in healthcare organisations," *Journal of Medical Internet Research (Preprint)*, vol. 25, p. In Press, 2023, https://doi.org/10.2196/41294.

[41] R. Rohan, S. Funilkul, D. Pal, and W. Chutimaskul, "Understanding of human factors in cybersecurity: A systematic literature review," in *International Conference on Computational Performance Evaluation (ComPE)*. Shillong, India: IEEE, 2021, pp. 133–140, 10.1109/ComPE53109.2021.9752358.

[42] A. Oltramari, D. S. Henshel, M. Cains, and B. Hoffman, "Towards a human factors ontology for cyber security." in *Proceedings of the Tenth Conference on Semantic Technology for Intelligence, Defense, and Security, Fairfax VA, USA, November 18-20*, 2015, pp. 26–33.

[43] R. van der Kleij and R. Leukfeldt, "Cyber resilient behavior: Integrating human behavioral models and resilience engineering capabilities into cyber security," in *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE International Conference on Human Factors in Cybersecurity, July 24-28*. Washington DC, USA: Springer, 2020, pp. 16–27, https://doi.org/10.1007/978-3-030-20488-4_2.

[44] N. Stembert, A. Padmos, M. S. Bargh, S. Choenni, and F. Jansen, "A study of preventing email (spear) phishing by enabling human intelligence," in *European Intelligence and Security Informatics Conference*. Manchester, UK: IEEE, 2015, pp. 113–120, https://doi.org/10.1109/EISIC.2015.38.

[45] W. Roden and L. Layman, "Cry wolf: Toward an experimentation platform and dataset for human factors in cyber security analysis," in *Proceedings of the ACM Southeast Conference*. Tampa, USA, April 2 - 4: ACM, 2020, pp. 264–267, https://doi.org/10.1145/3374135.3385301.

[46] M. Mehrnezhad, A. Ghaemi Bafghi, A. Harati, and E. Toreini, "PiSHi: click the images and I tell if you are a human," *International Journal of Information Security*, vol. 16, pp. 133–149, 2017, https://doi.org/10.1007/s10207-015-0311-z.

[47] L. Von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in *Eurocrypt*, vol. 2656. Warsaw, Poland: Springer, 2003, pp. 294–311.

[48] M. Belk, P. Germanakos, C. Fidas, G. Spanoudis, and G. Samaras, "Studying the effect of human cognition on text and image recognition CAPTCHA mechanisms," in *Human Aspects of Information Security, Privacy, and Trust: First International Conference, Held as Part of HCI International*. Las Vegas, NV, USA, July 21-26:

Springer, 2013, pp. 71–79.

[49] S. K. Sowe, E. Simmon, K. Zettsu, F. De Vaulx, and I. Bojanova, "Cyber-physical-human systems: Putting people in the loop," *IT Professional*, vol. 18, no. 1, pp. 10–13, 2016, https://doi.org/10.1109/MITP.2016.14.

[50] W. Sinlapanuntakul, C. M. Fausett, and J. R. Keebler, "Exploring team competencies in cybersecurity," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 66, no. 1, pp. 1110–1114, 2022, https://doi.org/10.1177/1071181322661496.

[51] J. Stella and M. Corry, "A capability approach for online primary and secondary students with disabilities," *British Journal of Special Education*, vol. 44, no. 4, pp. 448–464, 2017, https://doi.org/10.1111/1467-8578.12187.

[52] D. Gasper, "What is the capability approach? Its core, rationale, partners and dangers," *The Journal of Socio-Economics*, vol. 36, pp. 335–359, 2017, https://doi.org/10.1016/j.socec.2006.12.001.

[53] H. Ritchie, "The world population is changing: For the first time there are more people over 64 than children younger than 5," 2019, https://ourworldindata.org/population-aged-65-outnumber-children.

[54] R. Sun and Z. Zhang, "Leisure activities and cognitive impairment in old age: The role of life course socioeconomic status," *Aging & Mental Health*, vol. 27, no. 2, pp. 326–333, 2023, https://doi.org/10.1080/13607863.2022.2046694.

[55] Y. Uchida, S. Sugiura, Y. Nishita, N. Saji, M. Sone, and H. Ueda, "Age-related hearing loss and cognitive decline—the potential mechanisms linking the two," *Auris Nasus Larynx*, vol. 46, no. 1, pp. 1–9, 2019, https://doi.org/10.1016/j.anl.2018.08.010.

[56] J. Tao and H. Shuijing, "The elderly and the big data how older adults deal with digital privacy," in *International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)*. IEEE, 2016, pp. 285–288.

[57] P. Lošonczi, "Importance of dealing with cybersecurity challenges and cybercrime in the senior population," *Security Dimensions*, vol. 26, pp. 173–186, 2018.

[58] H. M. Mentis, G. Madjaroff, and A. K. Massey, "Upside and downside risk in online security for older adults with mild cognitive impairment," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*. Glasgow, UK: ACM, 2019, pp. 1–13, https://doi.org/10.1145/3290605.3300573.

[59] A. Frik, L. Nurgalieva, J. Bernd, J. Lee, F. Schaub, and S. Egelman, "Privacy and security threat models and mitigation strategies of older adults," in *Fifteenth Symposium on Usable Privacy and Security (SOUPS)*, 2019, pp. 21–40.

[60] T. Nef, R. L. Ganea, R. M. Müri, and U. P. Mosimann, "Social networking sites and older users–a systematic review," *International Psychogeriatrics*, vol. 25, no. 7, pp. 1041–1053, 2013, https://doi.org/10.1017/S1041610213000355.

[61] H.-Y. Huang and M. Bashir, "Surfing safely: Examining older adults' online privacy protection behaviors," *Proceedings of the Association for Information Science and Technology*, vol. 55, no. 1, pp. 188–197, 2018, https://doi.org/10.1002/pra2.2018.14505501021.

[62] A. Quan-Haase and I. Elueze, "Revisiting the privacy paradox: Concerns and protection strategies in the social media experiences of older adults," in *Proceedings of the 9th International Conference on Social Media and Society*, 2018, pp. 150–159, https://doi.org/10.1145/3217804.3217907.

[63] A. Quan-Haase and D. Ho, "Online privacy concerns and privacy protection strategies among older adults in East York, Canada," *Journal of the Association for Information Science and Technology*, vol. 71, no. 9, pp. 1089–1102, 2020, https://doi.org/10.1002/asi.24364.

[64] B. Knowles, V. L. Hanson, Y. Rogers, A. M. Piper, J. Waycott, N. Davies, A. H. Ambe, R. N. Brewer, D. Chattopadhyay, M. Dee, and D. Frohlich, "The harm in conflating aging with accessibility," *Communications of the ACM*, vol. 64, no. 7, pp. 66–71, 2021, https://doi.org/10.1145/3431280.

[65] United Nations. World Population Prospects 2022. https://population.un.org/wpp/Graphs/DemographicProfiles/Pyramid/1503.

[66] N. Alkaldi and K. Renaud, "MIGRANT: modeling smartphone password manager adoption using migration theory," *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, vol. 53, no. 2, pp. 63–95, 2022.

[67] S. Alkire and R. Black, "A practical reasoning theory of development ethics: furthering the capabilities approach," *Journal of International Development*, vol. 9, no. 2, pp. 263–279, 1997, 10.1002/(SICI)1099-1328(199703)9:2%3C263::AID-JID439%3E3.0.CO;2-D.

[68] P. Ralph, "ACM SIGSOFT empirical standards released," *ACM SIGSOFT Software Engineering Notes*, vol. 46, no. 1, pp. 19–19, 2021, https://doi.org/10.1145/3437479.3437483.

[69] Miro, "Miro | online whiteboard for visual collaboration," 2022, https://miro.com/.

[70] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, 2006, https://doi.org/10.1191/1478088706qp063oa.

[71] U. Schauberger, "Universal barriers to access," 2023, https://uteschauberger.com/barrierstoaccess.html.

[72] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor, "I added '!' at the end to make it secure: Observing password creation in the lab," in *Proc. SOUPS*. Ottawa, Canada: ACM, 2015, p. 123–140.

[73] E. Derr, S. Bugiel, S. Fahl, Y. Acar, and M. Backes, "Keep me updated: An empirical study of third-party library updatability on Android," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 2187–2200. [Online]. Available: https://doi.org/10.1145/3133956.3134059

[74] S. Ciolino, S. Parkin, and P. Dunphy, "Of two minds about two-factor: Understanding everyday FIDO u2f usability through device comparison and experience sampling," in *Symposium on Usable Privacy and Security (SOUPS)*. Santa Clara, USA: USENIX, 2019, pp. 339–356.

[75] S. Das, G. Russo, A. C. Dingman, J. Dev, O. Kenny, and L. J. Camp, "A qualitative study on usability and acceptability of Yubico security key," in *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*. Orlando, USA: ACM, 2018, pp. 28–39, https://doi.org/10.1145/3167996.3167997.

[76] M. O. Jewell, E. Costanza, and J. Kittley-Davies, "Connecting the things to the internet: an evaluation of four configuration strategies for Wi-Fi devices with minimal user interfaces," in *Proceedings of the International Joint Conference on pervasive and ubiquitous computing*. Osaka Japan: ACM, 2015, pp. 767–778, https://doi.org/10.1145/2750858.2807535.

[77] A. Alqahtani, "Usability testing of google cloud applications: Students' perspective," *Journal of Technology and Science Education*, vol. 9, no. 3, pp. 326–339, 2019.

[78] A. Sen, "The political economy of targeting," 1992, keynote Address In D. van de Walle and K. Nead, eds., Public Spending and the Poor (Washington, DC, World Bank 1995).

[79] C. Barber, "Notes on poverty and inequality," 2008, Oxfam International. https://oxfamilibrary.openrepository.com.

[80] K. Allmann, "UK digital poverty evidence review 2022," 2022, https://digitalpovertyalliance.org/uk-digital-poverty-evidence-review-2022/ Accessed 26 March 2023.

[81] A. K. Jones, "The object model: A conceptual tool for structuring software," in *Operating Systems: An Advanced Course*, R. Bayer, R. Graham, and G. Seegmüller, Eds. Berlin, Germany: Springer, 1978, ch. 2A, pp. 7–16.

[82] B. W. Lampson and H. E. Sturgis, "Reflections on an operating system design," *Communications of the ACM*, vol. 19, no. 5, pp. 251–265, 1976, https://doi.org/10.1145/360051.360074.

[83] S. J. Mullender and A. S. Tanenbaum, "The design of a capability-based distributed operating system," *The Computer Journal*, vol. 29, no. 4, pp. 289–299, 1986.

[84] J. Woodruff, R. N. Watson, D. Chisnall, S. W. Moore, J. Anderson, B. Davis, B. Laurie, P. G. Neumann, R. Norton, and M. Roe, "The cheri capability model: Revisiting risc in an age of risk," *ACM SIGARCH Computer Architecture News*, vol. 42, no. 3, pp. 457–468, 2014, https://doi.org/10.1145/2678373.2665740.

[85] C. Cremers, J. Fairoze, B. Kiesl, and A. Naska, "Clone detection in secure messaging: improving post-compromise security in practice," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. Virtual: ACM, 2020, pp. 1481–1495, https://doi.org/10.1145/3372297.3423354.

[86] P. Das Chowdhury, M. Sameen, J. Blessing, N. Boucher, J. Gardiner, T. Burrows, R. Anderson, and A. Rashid, "Threat Models over Space and Time: A Case Study of E2EE Messaging Applications," 2023, arXiv preprint arXiv:2301.05653.

[87] B. Christianson, "Auditing against impossible abstractions," in *International Workshop on Security Protocols*. Cambridge, UK: Springer, 1999, pp. 60–64.

[88] M. Tahaei and K. Vaniea, "A survey on developer-centred security," in *European Symposium on Security and Privacy Workshops (EuroS PW)*. Stockholm, Sweden: IEEE, 2019, pp. 129–138, https://doi.org/10.7488/ds/2535.

[89] M. Tahaei, J. Bernd, and A. Rashid, "Privacy, permissions, and the health app ecosystem: A stack overflow exploration," in *Proceedings of the European Symposium on Usable Security*. Karlsruhe, Germany: ACM, 2022, pp. 117–130, https://doi.org/10.1145/3549015.3555669.

[90] M. Tahaei, R. Abu-Salma, and A. Rashid, "Stuck in the permissions with you: Developer & end-user perspectives on app permissions & their privacy ramifications," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, ser. CHI '23. Hamburg, Germany: ACM, 2023, https://doi.org/10.1145/3544548.3581060.

[91] P. Das Chowdhury, J. Hallett, N. Patnaik, M. Tahaei, and A. Rashid, "Developers are neither enemies nor users: they are collaborators," in *IEEE Secure Development Conference (SecDev)*. Virtual: IEEE, 2021, pp. 47–55, 10.1109/SecDev51306.2021.00023.

[92] Y. Acar, M. Backes, S. Fahl, D. Kim, M. L. Mazurek, and C. Stransky, "You get where you're looking for: The impact of information sources on code security," in *Symposium on Security and Privacy (SP)*. San Jose, CA: IEEE, 2016, pp. 289–305, 10.1109/SP.2016.25.

[93] D. Van Der Linden, E. Williams, J. Hallett, and A. Rashid, "The impact of surface features on choice of (in)secure answers by Stackoverflow readers," *IEEE Transactions on Software Engineering*, pp. 1–18, Apr. 2020.

[94] A. Schlesinger, W. K. Edwards, and R. E. Grinter, *Intersectional HCI: Engaging Identity through Gender, Race, and Class*. New York, NY, USA: Association for Computing Machinery, 2017, p. 5412–5427. [Online]. Available: https://doi.org/10.1145/3025453.3025766

[95] J. Drèze and A. Sen, "Putting growth in its place," *Yojana*, vol. 56, pp. 36–40, 2012.

A SURVEY QUESTIONS

Introduction

We are going to present you with a number of scenarios Senior citizens might face and ask for your opinion about the challenges, difficulties and challenges they might face. All speak English. They are likely to have age-related impaired eye sight (not blindness) and physical disabilities as comparable to people of their age group.

When you read the scenario, think about the challenges/difficulties that the person would face in each scenario, and tell us about it. We would really appreciate comprehensive responses

We are not testing YOU - we are asking for your help in understanding the challenges and difficulties that Seniors might face.

We really appreciate comprehensive answers

Thank you!

Strong Passwords Scenario

Bob is a senior citizen in his early 80s. He has been using his computer for years to stay in touch with his family and manage his finances. Recently, his bank asked him to update his password for security reasons. Bob knows that this is an important account, so he wanted to make sure that he created a strong and secure password that would be difficult for hackers to guess.

Bob sat down at his computer and started to think about what kind of password he should use. He knew that he should not use his name or birth date. He also knew that he shouldn't use the same password for all his accounts.

What challenges and difficulties might Bob face in this situation?

Software Update Scenario

John is an 80-year-old retiree. He actively uses his brand new smartphone. He just received a message on his phone telling him that a software update is available.

What challenges and difficulties might John face in this situation?

Multifactor Authentication Scenario

Sadie is a senior citizen in her late 70s. She has been using her computer and smartphone to stay connected with her family and friends for years. Recently, she signed up for an online banking service. The bank requires her to use two- factor authentication to log in to her account.

(An example of Two-Factor authentication is when the bank sends a code to your phone for you to enter after you have provided your password).

What challenges and difficulties might Sadie face in this situation?

Secure WiFi Scenario

Karabo is a senior citizen in her mid-70s. She has been using the internet to stay connected for years. She has a wireless router in her home that allows her to connect to the internet with her laptop and smartphone.

She recently learned that her neighbors have been accessing her WiFi network without her permission. Karabo is concerned about her privacy and security, so she wants to secure her WiFi network. She did some research and learned that there were several steps she could take.

What challenges and difficulties might Karabo face in this situation?

Make Backups Scenario

Lindiwe is a 65-year-old woman who loves taking photos of her family and friends. She has accumulated quite a collection of precious memories. However, Lindiwe is worried about losing these photos. To protect her photos, Lindiwe decides she needs to back them up.

What challenges and difficulties might Lindiwe face in this situation?

Thanks

Our research is related to technology use by Seniors, specifically cybersecurity (as you may have surmised).

If you have anything to add that you think we should know about, please use this space to tell us.