Beyond "Vulnerable Populations": A Unified Understanding of Vulnerability From A Socio-Ecological Perspective

XINRU TANG, University of California, Irvine, USA
GABRIEL LIMA, Max Planck Institute for Security and Privacy, Germany
LI JIANG, George Washington University, USA
LUCY SIMKO, Barnard College, USA
YIXIN ZOU*, Max Planck Institute for Security and Privacy, Germany

HCI and CSCW research has witnessed increasing efforts to address diversity and inclusion in research and design practice, as evidenced by the growing body of research with populations deemed as vulnerable, marginalized, or underserved. However, this work has been largely limited to a population-specific approach, i.e., identifying certain populations as vulnerable and gathering their individual experiences. Drawing primarily from human-centered security and privacy research, we identify three key challenges faced by this population-specific approach: (1) It is limited in addressing user diversity within the target population; (2) It may fail to capture the complex social reality of vulnerability; and (3) It runs the risk of perpetuating othering and stereotypes. To address these limitations, we propose a socio-ecological perspective on vulnerability adapted from the Ecological System Theory (EST). We argue that a socio-ecological perspective of vulnerability can guide researchers to look beyond static and stigmatizing definitions of vulnerability — instead, focus on the situations, relations, and structures that lead to vulnerability, eventually enabling transferable knowledge of vulnerability across populations. We demonstrate how the socio-ecological lens maps onto existing work and generates new insights in the case of older adults' security and privacy, as well as its potential for being applied to other contexts such as reproductive privacy and responsible artificial intelligence. We end by providing concrete recommendations on how HCI and CSCW research can better operationalize vulnerability in scholarship and design practice.

CCS Concepts: • **Human-centered computing → HCI theory, concepts and models**.

Additional Key Words and Phrases: vulnerable populations, inclusion, diversity, human-centered security and privacy, Ecological Systems Theory

ACM Reference Format:
Xinru Tang, Gabriel Lima, Li Jiang, Lucy Simko, and Yixin Zou. 2025. Beyond "Vulnerable Populations": A Unified Understanding of Vulnerability From A Socio-Ecological Perspective. *Proc. ACM Hum.-Comput. Interact.* 9, 2, Article CSCW037 (April 2025), 30 pages. https://doi.org/10.1145/3710935

*Corresponding author

Authors' Contact Information: Xinru Tang, University of California, Irvine, Irvine, California, USA, xinrut1@uci.edu; Gabriel Lima, Max Planck Institute for Security and Privacy, Bochum, Germany, gabriel.lima@mpi-sp.org; Li Jiang, George Washington University, Washington, D.C., District of Columbia, USA, lijiang1@email.gwu.edu; Lucy Simko, Barnard College, New York City, New York, USA, lsimko@barnard.edu; Yixin Zou, Max Planck Institute for Security and Privacy, Bochum, Germany, yixin.zou@mpi-sp.org.

ACM 2573-0142/2025/4-ARTCSCW037
https://doi.org/10.1145/3710935

1 Introduction

The concept of *vulnerable populations* has profoundly shaped the inclusion and social justice discourse. Typically referring to groups at heightened risk of disproportionate harm and exploitation in society [38, 94, 227], this term has been central to promoting inclusion within regulatory frameworks and ethical principles since the 1940s. It has shaped areas such as human subject research [38], humanitarian programs [94], and legal protections [227], establishing the need for additional attention and care for specific groups, such as children in privacy protection [70] and low-income populations in healthcare [191].

The HCI and CSCW communities have embraced the growing call for diversity and inclusion, as evidenced by concepts and frameworks such as feminist HCI [16], HCI for development [46] and justice-oriented interaction design [52]. However, similar to broader inclusive efforts, much of this work relies heavily on a *population-specific* approach, which usually involves two components: (1) identifying certain populations for the goal of inclusion, often interchangeably using terms such as vulnerable populations [93, 144, 203] and at-risk users [19, 212]; (2) developing population-specific knowledge and proposing countermeasures accordingly. For example, the growing inclusive efforts in human-centered security and privacy (S&P) research are driven by collecting data about the experiences and behaviors of specific groups of people, as identified in a recent review [167]. Although population-specific studies contribute insights into specific individuals' and communities' experiences, we identify three key challenges in relying on this approach:

- **Addressing user diversity within the target population.** Heterogeneity always exists within the target population. Some prior work has focused on smaller groups with intersectional identities, such as blind and low-vision older adults [28, 61, 161]. However, relying on a focus on populations with intersecting categories may risk splitting groups along the lines of categories or creating arbitrary intersections [111]. We need research methodologies to better recognize and address individual differences within demographic groups.
- **Theorizing the complex social reality of vulnerability.** Although population-specific studies yield rich empirical insights into particular groups, by this approach alone, we are still missing a unified and structural understanding of needs and practices across populations [167]. Recently, some taxonomies have attempted to identify shared experiences across populations such as in the context of privacy [130, 212]. However, we argue that these taxonomies may imply a rigid and static structure for defining vulnerability, overlooking the dynamic relations and structures that shape human experiences. Research will benefit from alternative vulnerability models to better capture its complexity and dynamics.
- **Avoiding perpetuation of othering.** Framing individuals as members of a vulnerable population might imply their experiences are distinct and irrelevant to the broader population and disempower them when facing oppression [218]. Harms could further occur when researchers consistently associate vulnerability with specific populations [120] in ways that perpetuate stereotypes without recognizing contextual factors that cause those vulnerabilities [110].

To tackle these challenges, we introduce a socio-ecological view of vulnerability adapted from the Ecological Systems Theory (EST) [29], as a starting point for shaping future research and practice around inclusion. **We argue that vulnerability should not be viewed as a fixed characteristic of individuals or groups, but as a complex multi-layered socio-ecological system that changes over space and time.** Instead of using "vulnerable" to label certain populations, vulnerability should be studied as a multi-layered system shaped by interactions between individuals and systems surrounding them at different layers, such as family, community, and socio-cultural environments. Each of these layers plays a role in shaping vulnerability, with all of them interacting and evolving over time. Using S&P research with older adults as a case study, we explore how

the socio-ecological lens can enrich understanding and inform future research directions around inclusion, and how this lens could transfer to other contexts such as reproductive privacy and responsible artificial intelligence.

By positioning the socio-ecological view of vulnerability, we hope it can serve as a unified framework for theorizing inclusion across populations from the lens of human vulnerability. Our goal is to propose a new perspective of conceptualizing vulnerability as a type of theoretical contribution — one of the main research contributions in HCI defined by Wobbrock that typically include "new or improved concepts, definitions, models, principles, or frameworks" [217]. In developing the socio-ecological view of vulnerability, we tried to ground it in prior literature as much as possible. That being said, we do not intend to provide a systematic review of vulnerability in HCI and CSCW research, as prior HCI work focusing on theoretical contributions such as Chen et al. on trauma-informed computing [36], Dombrowski et al. on social justice-oriented design [52], and Im et al. on affirmative consent [96], similarly did not adopt the systemization of knowledge (SoK) approach. However, some SoK work [130, 167, 212] greatly influenced our ways of thinking for this work.

What do we mean by vulnerability? Prior research has used different concepts as the goal for inclusion, including justice [35], fairness [8], equity [59], and power [35, 162]. To identify groups for the goal of inclusion, research has used terms such as "disadvantaged" [204], "marginalized" [116, 167], "at-risk" [19, 212], "stigmatized" [125], "underserved" [51], and "underrepresented" [49]. These terms reflect different goals or rationales for inclusion. Some terms refer to the ideal yet abstract goals of inclusion. Others emphasize social inequalities or highlight the disproportionate risks and harm people may experience under certain conditions. Despite the term differences, we believe research along this line shares similar goals of ensuring everyone has equal opportunities to participate in society.

We focus on the terms *vulnerable populations* and *vulnerability* to capture the diverse expressions that previous research has used to identify user groups and conditions for the purpose of promoting inclusion. Past research has employed other terms interchangeably, such as at-risk users [19, 212] and marginalized groups [167] to convey similar ideas. We anchor our paper on *vulnerability* because we see its potential as a universal concept to advance inclusion. We refer to the Cambridge Dictionary for a basic definition of *vulnerability* — "the quality of being susceptible, i.e., being able to be easily hurt, influenced, or attacked" [50]. According to this definition, everyone could experience vulnerability, be it an emotional feeling or sensitive information to protect from others — as illustrated by Calo's example of Superman and Lex Luthor [32].

The scope of our work. In developing our arguments, we primarily draw from human-centered S&P research [68] — research that sits at the intersection of HCI and computer S&P — since the area represents a typical HCI sub-area having a growing interest in inclusion [209, 210], and recent SoKs in this area have sought to consolidate findings across different at-risk users [19, 212] and marginalized groups [167]. While we attempt to show a more nuanced overview of vulnerability (Section 2) and transferability of this work in other contexts (Section 6), we need to explicitly acknowledge our work's grounding in S&P research. Additionally, while we tried to include information and communication technology for development (ICT4D) literature, most of our references are based on samples in Western, Educated, Industrialized, Rich, and Democratic (WEIRD) contexts. This representation is largely a by-product of the fact that HCI and usable S&P research is primarily based on knowledge and values produced by people in WEIRD societies [83, 121].

Positionality. Our team consists of five academic researchers, four in HCI/CSCW and one in behavioral economics. While we have multicultural backgrounds from Brazil, China, and the United

States, we all work in academic institutions in North America and Europe and are most familiar with research conducted in these contexts. We specialize in various topics, including accessibility and aging, responsible artificial intelligence, and S&P. Many of us have directly engaged with traditionally identified vulnerable populations in research.

2 Background and Related Work

We summarize the historical origin of the concept of *vulnerability* and how the term has been used in research ethics and real-world practice. We then review how the term is translated into HCI, CSCW, and S&P research. Our knowledge of *vulnerability* and *vulnerable populations* is based on a wide range of areas, including research ethics, legal frameworks, and empirical studies across diverse fields. Considering this paper is mainly positioned for HCI, CSCW, and S&P audiences, much of the knowledge is drawn from related venues. While we aim to provide a comprehensive overview, this review is not intended to be exhaustive.

2.1 The Origin and Role of "Vulnerability" in Research and Regulations

Vulnerability has served as a cornerstone concept in both ethics and regulations, shaping research and practice involving human beings [5, 38, 70, 77, 94, 154, 205]. The term's early appearances can be traced back to the establishment of ethical research principles for human experimentation, such as the Nuremberg Code of 1947 [150], the Declaration of Helsinki of 1964 [12], and the Belmont Report of 1979 [151]. All these documents mandated informed consent as the major protection against research-caused harms, and the latter two specified that *vulnerable groups* warranted additional care. While initially focused on medical research, these ethical principles have made their way to other contexts [152]. For example, the Menlo Report of 2012 reinforces the importance of informed consent in information and communication technology research, posing that people incapable of giving informed consent should be entitled to protection [152]. Besides research, *vulnerability* has also been a key term in real-world practice with crucial consequences, such as in humanitarian aid programs [5, 77, 94] and in consumer protection laws and regulations [70, 101, 154, 205].

Despite its frequent use, the term has been criticized for being too broad to be useful [38, 75, 124], and there is limited consensus on how to enforce the associated principles [38, 75]. For instance, in the U.S., despite being the focal document of the U.S. human subject protection regulations, the Common Rule does not define vulnerability and offers little guidance on how Institute Research Boards should respond [38]. Similarly, consumer protection laws in the European Union define the average consumer as people who are "able to make rational choices to find the best deals and benefit from competitive markets" [227], whereas *vulnerable consumers* lack this capacity [54, 101, 227]. However, the implementation of this distinction can be ambiguous. In practice, vulnerability is often operationalized by identifying populations considered more vulnerable than others [56, 101, 227]. For example, the General Data Protection Regulation (GDPR) in the European Union listed children as an example when mentioning vulnerable natural persons [70].

However, the approach of listing specific vulnerable populations has been criticized for being too static, simple, and vague [75, 122, 123] even though it often comes with the disclaimer that the list is not exhaustive. Many scholars advocated for a deeper understanding of vulnerability to make it useful for analysis and practice in various contexts such as healthcare [47, 76, 106, 115, 122–124, 175], privacy [32], law [62], and finance [166]. For example, Coleman argued that research ethics review should differentiate types of vulnerabilities, such as consent-based versus risk-based vulnerability, and tailor protections accordingly [38]. Others argued that vulnerability should be based on situations rather than personal traits [149, 227], and practices like collecting personal data will make all consumers vulnerable [64, 227]. Due to the ambiguity of the concept, some policies chose to involve careful human assessment when identifying vulnerable groups. For example, the

United Nations provides a vulnerability assessment tool for screening refugees [5]. These ongoing debates and diverse practices reveal *vulnerability* as a complex and multifaceted concept that requires a nuanced and holistic understanding.

2.2 "Vulnerability" in HCI and CSCW

The concept of *vulnerability* has also played a key role in HCI and CSCW research and ethics, emphasizing that populations who are easier to experience harm require additional care and attention in research and design [69, 98, 170, 191, 215]. For example, Stowell et al. emphasize that some populations "disproportionately experience barriers to wellness" [191]. Scheuerman et al. included vulnerability as a dimension to evaluate the severity of online harmful content, emphasizing that certain populations may experience more severe harm caused by online content, such as children [170]. There have been several workshops and panels for discussing challenges and considerations in research and design with *vulnerable populations* [35, 93, 132, 214].

Nevertheless, similar to the broader discussions on *vulnerability* mentioned in Section 2.1, the definition and use of the term remains unclear in HCI and CSCW. Vulnerability is often associated with certain populations, but the specific context — being health informatics [191], user interface design [93], or S&P [212] — also adds nuances to the understanding. For example, Stowell et al. focused on low-socioeconomic, racial/ethnic minorities, and people living with disabilities in their systematic review of mobile health interventions for vulnerable populations [191]. By contrast, in the context of digital cybersecurity, Warford et al. defined at-risk users as people experiencing "risk factors that augment or amplify their chances of being attacked digitally and/or suffering disproportionate harms from an attack," covering populations like activists, teachers, and journalists [212]. Recognizing the diverse manifestations of vulnerabilities, Pierce et al. introduced the notion of differential vulnerability to challenge vulnerable populations as a pre-existing category in the context of cybersecurity [159]. As they noted, people experience different types of vulnerabilities positioned in relations; the questions that matter to research should be "Who is vulnerable to what?" and "Who applies the label of vulnerable?" [159].

In contrast to population-specific definitions, some HCI and CSCW research recognized vulnerability as a common human experience or feeling. For example, Barta et al. developed a taxonomy of sources and causes of vulnerability people experience on social media [18]. One of their key arguments is that vulnerability is situational, and platform affordances take responsibility for enabling or perpetuating vulnerability [18]. Other HCI and CSCW research has similarly argued that vulnerability could be caused or amplified by design features and platform governance models [36, 160, 174]. For example, the trauma-informed computing framework shows how trauma, a common emotional state of vulnerability, can be caused by designs inconsiderate of people's traumatic experiences, such as when security warnings cause retraumatization to survivors of tech-enabled abuse [36, 176]. Nevertheless, some scholars argued against using vulnerability too broadly as such because it may ignore the structural barriers and social inequalities some populations experience [98]. These divergent viewpoints emphasize the need for more discussions around vulnerability to improve its clarity and practicality to guide HCI and CSCW research.

2.3 "Vulnerable Populations" in Usable Security and Privacy Research

Since Wang introduced inclusive privacy as the third wave of usable S&P research [209, 210], the S&P research community has paid increasing attention to people who are traditionally ignored in S&P designs, such as "children, older adults, people with disabilities, activists, journalists, victims of crimes or domestic violence, and people from non-Western or developing countries" [210]. Although Wang and his colleagues mainly focused on blind and low-vision people [14, 86, 104], more efforts since then have pushed usable S&P research to include more diverse populations in terms of

(dis)abilities, cultures, and life situations [167, 212], highlighting people's diverse S&P needs and challenging the idea of an average or general user [159]. As one step further, McDonald and Forte argued that vulnerability should even be at the core of privacy theorizing to raise awareness of power differentials in shaping privacy theories and norms [133].

Some recent usable S&P research goes further by synthesizing existing findings across different populations [130, 167, 212]. For example, Warford et al. synthesized findings from 95 papers, identifying 31 at-risk populations based on categories such as age, occupation, gender, ability, living areas, socio-economic status, social relationships, life situations, and their intersections; they also summarized three major risk factors: societal factors relationships, and personal circumstances [212].

Despite the growing awareness and existing systematization efforts, usable S&P research could still benefit from a unified understanding of vulnerability, as most prior work has focused on populations based on hard-coded identities and demographics, particularly disability [167]. Recent research has called for a more holistic analysis of root causes of exclusion, such as social structures, histories, and policies [162, 167, 192]. For example, Redmiles et al. argued that when designing and implementing systems, S&P researchers should be aware of the prevalent power structures — relationships between the protectors and the protected [162]. Similarly, Strohmayer et al. encouraged examinations into broader systems of oppression that affect everyone — such as "racism, sexism, ableism, heterosexism, and classism" — as necessary considerations for building safe technologies [192]. Some empirical studies also support that vulnerability goes beyond hard-coded identities and demographics. For example, Simko identified change as a natural cause of security vulnerability, as S&P tools frequently fail to meet people's evolving needs during significant changes such as immigration and natural disasters [181]. Building on these existing critiques of usable S&P research, we provide a critical analysis of vulnerability in current S&P research and introduce the socio-ecological perspective as an alternative way for conceptualization and systematic operationalization.

3 Key Challenges of Population-Specific Studies

We identify three key challenges faced by the population-specific approach adopted in inclusion research: (1) how to address user diversity within the target population, (2) how to capture the complex social reality of vulnerability, and (3) how to tackle ethical tensions in naming certain populations as vulnerable.

3.1 User Diversity Within the Target Population

Drawing population-specific conclusions always raises questions about diversity within populations. Crenshaw coined the concept *intersectionality* to emphasize that human experiences are the result of intersecting contexts [41]. D/deaf[1] women, as an example, encounter distinct forms of intimate partner abuse compared to their hearing counterparts: abusers may use their hearing- and/or gender-based privileges to isolate d/Deaf women, while d/Deaf women might grapple with concerns about seeking support from hearing-dominated institutions [7]. The marginalization of this population comes from both hearing- and masculinity-based domination in societies. Heterogeneity within the target population also means that individuals from a population that is traditionally viewed as vulnerable may not think they are more vulnerable than others. For example, some older adults are highly tech-savvy and do not think they are more vulnerable to scams than younger people [226].

While HCI and CSCW research has paid increasing attention to intersectionality, existing research still tends to address intersectionality through a population-specific approach. Intersectionality is

[1]The lower case "deaf" often refers to the audiological condition of not hearing, whereas the uppercase "Deaf" often emphasizes one's cultural identity of being part of the Deaf community [157].

often translated into the representation of individuals with intersecting identities and populations in intersectionally marginalized contexts [155, 173]. However, as Kong observed, if researchers only focus on population representativeness, this approach will either keep splitting subgroups into smaller buckets or create arbitrary user groups according to pre-established categories (such as age, race, gender, and ability) while never fully addressing or acknowledging intersectionality [111]. In practice, characterizing particular populations as vulnerable may even hinder effective protection because people may have to concentrate on a small number of pre-defined categories due to resource constraints [89], even if the characteristics cannot fully represent the needs of the end user [57, 156].

3.2 The Complex Social Reality of Vulnerability

When advancing and broadening knowledge on vulnerability, HCI and CSCW research has often focused on collecting unique experiences from target communities [167] while using taxonomies to augment and scale up findings across populations [130, 167, 212]. However, the complexity and variance of vulnerability can pose epistemological challenges to this approach of scaling through taxonomies.

Originating from biology, a taxonomy is centered on constructing classification systems for grouping and categorizing entities [74], implying a rigid and static structure. Yet, real-life vulnerability is far more nuanced than what can be captured by an orderly list of risk factors [134, 179, 198, 224]. Taking abuse survivors as an example, their specific S&P needs could vary depending on the stakeholders they interact with (being social workers, law enforcement, or tech support professionals) [66, 224], whether the support is provided in person or remotely [198], or whether the survivor experiences other forms of marginalizations such as being deaf or hard-of-hearing [7]. These nuances across individuals and situations could be overlooked in taxonomies where abuse survivors are universally labeled as a vulnerable population [130, 212]. While one may argue that taxonomies can be crafted for various populations and scenarios, achieving a systematic and clear classification through taxonomies would be challenging given the intricate and varying nature of vulnerability [123].

In addition, taxonomies of specific risk factors and harms are often constrained by the dimensions they focus on. For example, Warford et al. identified risk factors along the societal, relational, and personal dimensions [212]. A possible critique is that vulnerability should not be equated to risk factors, or risk factors alone are not enough to cause harm. Building on this critique, McDonald and her colleagues identified the mechanisms that turn risk factors into harms such as treating identities as being hard-coded [130]. Expanding on these efforts, we provide a framework to explain the interactions of different risk factors in the broader structures in Section 4.

3.3 Othering

Treating certain populations as inherently and persistently vulnerable may further reinforce existing power structures and promote stigmatization [110, 133, 219]. Link and Phelan identified stigmatization as a four-stage social process that involves labeling, stereotyping, separating, and status loss [119]. Classifying certain groups as vulnerable populations can map to this process.

As an area with a long history of battling stigmatization, disability studies have long emphasized the oppression behind naming, such as by differentiating between what is "normal" and "abnormal" [44, 120]. Echoing these efforts, the accessibility research community has been advocating for the use of inclusive language [1, 180]. For example, the accessibility and aging subcommittee of CHI2024 specifically listed "vulnerable" as a word that should be avoided [1]. Recent HCI work has also advocated for shifting the focus from deficits and limitations to recognizing strengths of marginalized communities [196, 219], such as through assets-based design approaches [219]. Some scholars further acknowledged both pains and hopes as normalized parts of human life, arguing for

understanding complexity, contradiction, and the self-determination of human living [129]. Tuck has referred to this perspective as a "desire-based framework" [199].

In fact, the inclusion criteria of vulnerable populations often seem unclear from existing taxonomies such as Warford et al. [212]. Drawing from European Union consumer protection laws and the definition of an average consumer [227], the baseline for comparison could be a digitally literate and rational person who can protect themselves from harm to their interests. Nonetheless, empirical evidence from behavioral economics research suggests that such an ideal user is often an illusion [3]; instead, people's privacy decision-making is uncertain, context-dependent, and malleable [2]. Hence, some scholars argue that vulnerability should be a more universal concept as part of human existence [32, 62].

4 Theorizing Vulnerability as a Socio-Ecological System

We propose a socio-ecological view of vulnerability drawing from the Ecological Systems Theory (EST) [29] as an alternative way of conceptualizing vulnerability. As discussed in Section 3, there are challenges when operationalizing vulnerability through static, simplistic, and rigid population-specific labels and taxonomies. We present the socio-ecological view to introduce a more dynamic, open, and intricate structure for understanding vulnerability. We identify the Ecological Systems Theory (EST) as a suitable theoretical foundation as it offers insights into the complex human relationships with surrounding environments [29]. Similar to other concepts and frameworks in HCI [16, 96], we believe our socio-ecological view of vulnerability has both explanatory and generative power: it can be used to unify existing understanding of people's vulnerable experiences and to generate new ideas and principles. After introducing the EST (Section 4.1), we show how the socio-ecological view can better explain vulnerability in HCI, CSCW, and S&P research (Section 4.2) as well as generate principles for a more nuanced analysis and operationalization of vulnerability (Section 4.3).

4.1 Ecological Systems Theory (EST)

The EST framework was first proposed in developmental psychology [29]. The core idea is that humans are surrounded by a multi-layered socio-environmental system that evolves over time. More specifically, the framework comprises four nested layers that form the ecology of human development, with individuals situated at the center [29]. (1) The microlayer involves the most closely involved ties, such as family members, friends, and peers. (2) The exolayer encompasses indirect institutional influences, such as those from community organizations and service providers. (3) The macro layer consists of the broader sociocultural systems of societal norms and ideologies. (4) On the outermost layer, the EST includes a temporal layer that considers changes in socio-environmental systems throughout life courses.

The EST framework has been widely used in HCI, especially health informatics, as a theoretical framework to illustrate the surrounding socio-environmental systems that should be considered when designing support systems related to fertility [40], autism [11], and mental health [146]. The EST has also been applied to S&P research but to a much lesser degree. For example, Kumar et al. applied the EST to identify design opportunities for S&P aspects of classroom technology use [113]. Inspired by the EST, we propose viewing vulnerability as a socio-ecological system situated in interconnected relations. Figure 1 presents a rough view of vulnerability from a socio-ecological perspective in the context of S&P.

4.2 Vulnerability As a Socio-Ecological System

The socio-ecological view explains the diversity of vulnerability by conceptualizing it as a dynamic outcome within a multi-layered social ecosystem. Under this lens, vulnerability is dynamically

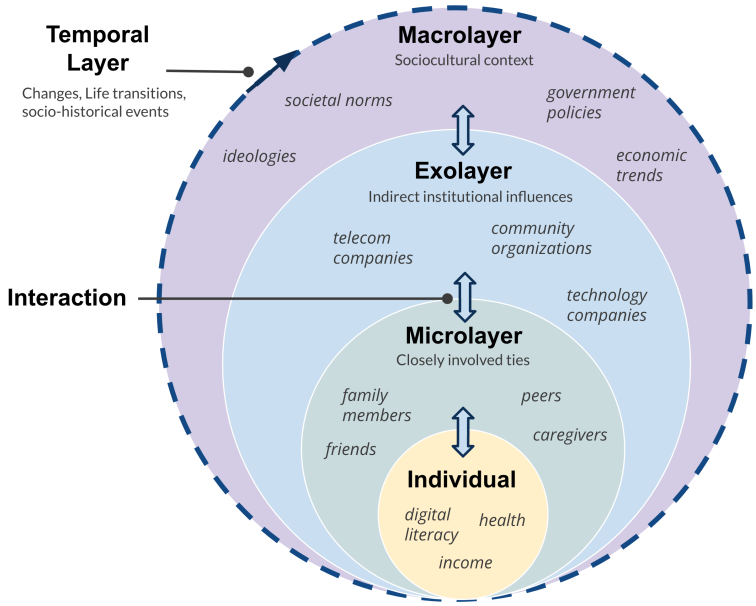

Fig. 1. We propose a socio-ecological framework of vulnerability adapted from the EST framework [29, 146]. The figure presented is an example of applying the EST framework in the context of S&P. Factors within each layer are non-exhaustive examples. This illustration is inherently incomplete and requires empirical research for validation and refinement.

shaped by the relationships between individuals and the interconnected system of social circles, communities, organizations, and institutions that surround them. This systemic thinking ties to the notion of *layered vulnerability* proposed by Luna [122–124], who argued that the metaphor for vulnerability should not be a label but layers.

The layered thinking approach addresses the diversity challenge inherent in population-specific frameworks by putting human vulnerability under the metaphor of *layers* — everyone is vulnerable, but vulnerability may vary because of different compositions of layers. For example, older adults with late-life vision impairments face complex challenges in technology use because of ongoing changes in different layers such as visual abilities, software, and accessibility tools [161]. Conversely, individuals from traditionally vulnerable demographics may not necessarily experience augmented vulnerability, for instance, when they cultivate digital competence [219, 226] or have resources and support from family members [195].

As such, the socio-ecological view conceptually offers a more organic, holistic, and flexible structure when compared to static structures such as taxonomies for explaining vulnerability. Under this view, vulnerability is a dynamic result shaped by complex, multi-layered, and changing structures concerning everyone rather than an objective entity that can be ordered into a classification system. The soft structure partly explains why it is challenging to use taxonomies to interpret vulnerability, as individuals often undergo complex forms of vulnerability shaped by numerous interacting layers that also evolve over time [198, 224].

Ethically, by putting everyone into the framework, the socio-ecological view avoids making assumptions about existing fixed categories of vulnerable populations and refraining from inappropriate generalizations from study participants to others. Rather, it focuses on theorizing the

hidden structures and mechanisms that lead to vulnerability in the first place. Layers may involve the population being studied but also other individuals more generally. For example, deceptive design patterns introduce vulnerability to everyone.

By incorporating a temporal layer, the socio-ecological perspective further normalizes vulnerability as a natural aspect of the human experience, acknowledging that everyone faces changes and uncertainties throughout life. Aging, for example, is a universal process that can introduce vulnerability to all individuals. Vulnerability can also arise from deliberate, context-specific choices; for instance, self-disclosure could be an informed decision resulting in expected vulnerability [18, 221].

4.3 Unpacking the System of Vulnerability

In addition to explaining the intricacies of vulnerability, we see the socio-ecological view's potential for suggesting additional directions to be prioritized in future research. First, the socio-ecological view breaks down vulnerability into layers, clarifying how vulnerability is situated in interconnected systems. Second, the socio-ecological view reveals time as an important dimension for deconstructing vulnerability. Along these two dimensions, we believe that future research can better theorize and operationalize the situations, relations, and patterns that give rise to vulnerability in a more inclusive way.

4.3.1 Unpacking the Layers of Systems. One can unpack the system of vulnerability layer by layer to explain the variance of vulnerability among individuals — individuals at the center, and the surrounding micro, exo, and macro layers. First off, we situate individuals at the core of the framework. As evidenced by many population-specific studies, individual characteristics such as income, education, and (dis)ability indeed shape individuals' use of technologies [82]. Individuals also play a crucial role in managing their vulnerability through actions such as self-disclosure [18] and deciding which technologies to trust [107].

However, when interpreting individuals' attributes and actions, they should be situated in complex social structures consisting of micro, exo, and macro layers. The *micro layer* encompasses the closest social ties, including family members, friends, peers, and caregivers. They often provide crucial support, such as in the case of younger family members supporting older adults [147, 195], but they can also be attackers, such as in the case of intimate partner abuse [65, 198]. The *exo layer* comprises institutional entities that are indirectly linked to individuals, including technology companies, community organizations, and service providers. For instance, there is already rich evidence supporting that many vulnerabilities are caused by designs rather than individuals themselves [42, 181, 184], such as in the case of dark patterns [207]. The *macro layer* functions as an overarching layer, which consists of high-level structures such as societal norms, ideologies, government policies, economies, and histories. For instance, privacy norms and people's perceptions of privacy are inherently embedded in cultures [147, 211] and government policies [42, 182]. In some cultures practicing filial piety, people may have the norm of sharing technological devices in families [147, 195] and not perceive it as a violation of privacy [195].

The layered approach inspired by the socio-ecological view could be used to unpack vulnerability more holistically and structurally when zooming into specific empirical studies. For instance, Simko et al. presented a case study showing how cultural assumptions embedded in privacy and security tools developed within U.S. contexts frequently pose barriers to refugees and amplify their vulnerability, such as by forcing the use of birthdays as authentication methods [182]. In this case, vulnerability does not come from the inabilities of the refugees but the misfits between refugees' needs and the technologies designed for them; these misfits could be further attributed to cultural assumptions situated at the macro layer and design practices at the exo layer.

Compared with the population-specific approach to vulnerability, a strength of the socio-ecological view is to examine all sources of vulnerability together while acknowledging their interactions. While the vulnerability examined in the case of refugees can be mostly traced back to the exo and macro layer, the resulting vulnerabilities for each individual will still take diverse forms due to the intricate layered social structures surrounding them, ranging from the supporters or attackers at the micro layer and personal attributes at the individual layer. We encourage future research to consider the whole systems of vulnerability for the problems they target. We give a more concrete example of applying our framework to older adults in Section 5.

4.3.2 Unpacking Vulnerability in Time. The temporal layer in the socio-ecological view introduces a more generative view of vulnerability. It acknowledges that vulnerabilities within all layers can emerge and evolve over time, coming from life transitions such as immigration, political activism, crisis time [42, 181–183], as well as individual actions such as self-disclosure [213] and incidental or unauthorized sharing [24]. These examples show that vulnerability can arise at any moment for any individual rather than being exclusive to certain populations.

Considering the temporal layer, research should be more cautious about the key moments and temporal patterns that shape vulnerability as the particular moment and duration of technology use may shape different patterns of vulnerabilities. For example, using a public device may introduce S&P vulnerability for end users, but individuals may need tailored protective strategies if they only use the device for a brief period, as seen in cybercafes [145]. Vulnerability can also be caused by temporary circumstances. For instance, tourists may be temporarily vulnerable due to their language skills [101].

Consequently, taking vulnerability as a static construct [135, 169] can lead to overproblematic assumptions and also overlook the resilience that individuals develop over time [135, 169] as well as certain types of vulnerabilities. For example, in the case of financial vulnerability, resource volatility, rather than static levels of income and wealth, may be more accurate measures for financial vulnerability [166]. As another instance, McHugh et al. found that risk exposure contributes to teens' mental well-being, but only in the short term [135]. However, as noted by prior work [18, 166, 168], risk and harm are still often conflated and taken as static constructs in HCI and CSCW research. By incorporating a temporal layer in analysis, the socio-ecological view can emphasize a more dynamic and fluid analysis of vulnerability.

5 Case Study on Older Adults

Bardzell argued that researchers should reflect on why HCI would benefit from a specific theory when researchers introduce it from another field or propose it themselves [15]. Being aware of this critique, we take older adults — who are traditionally defined as a vulnerable population in S&P research — and reflect on how our proposed socio-ecological view of vulnerability can advance existing understanding and inform future research with this population.

We chose to focus on older adults in our case study because this population has been featured prominently in HCI, CSCW, and S&P research that attempts to achieve inclusion. Besides, research has traditionally portrayed older adults through a deficit lens [67, 118, 203] by characterizing older adults as having limited technological literacy [6], being particularly vulnerable to S&P threats [6, 112, 147], and being easy targets of digital attacks [88, 136]. However, other research has shown significant variance in technology skills within this population [82] and older adults' rejection of technologies can be an informed choice rather than the result of lacking abilities and knowledge [109]. Consequently, there is an increasing call to refrain from harmful labeling related to this population and recognize within-group heterogeneity [82, 110, 143, 226].

Aligning with these calls to action, we discuss how the socio-ecological view of vulnerability can explain and unify existing research with older adults (Section 5.1) and generate avenues for future research that advances inclusion for older adults (Section 5.2).

5.1 Explanatory Insights from the Socio-Ecological View

The socio-ecological view of vulnerability can first function as a conceptual tool to unite the diverse findings across specific studies with older adults, providing a foundational understanding for future studies. From a layered perspective, there are factors at play at the individual level, ranging from cybersecurity awareness [143, 226], digital literacy [82, 143, 226], to stress [143] and financial conditions [82, 143]. However, even for older adults falling under the same category, they might experience different types of vulnerabilities under different compositions of the layers, such as social norms at the macro layer [195], platform designs at the exo layer [33, 114, 194], and availability of support at the micro layer. Furthermore, research has highlighted the relevance of the temporal layer by recognizing aging as a process of ongoing adaptation, including navigating technological advancements and significant life events [17, 26, 161].

By focusing on individual factors or systems within an exclusive layer, research may risk reinforcing a fragmented view of older adults' experiences and lead to designs that do not match the complexities of social reality experienced by each individual. For example, focusing on the micro layer, prior research raised the concern that family members managing technology for older adults may amount to paternalism [147]. However, in cultures that practice filial piety, family involvement, as controlling as it might seem, could be a natural part of technology adoption [80, 195]. Yet, even within these cultures, older adults might personally prefer less family involvement depending on family dynamics and personal preferences [195]. These mixed results exemplify the need to consider the macro layer (cultural norms), micro layer (family dynamics), and factors at the individual level (personal preferences) simultaneously to achieve a more holistic understanding of each individual's experience, especially when proposing interventions and solutions to individuals.

5.2 Generative Insights from the Socio-Ecological View

Beyond unifying existing research, the socio-ecological view of vulnerability can help pinpoint crucial knowledge gaps and guide future research with older adults in the context of S&P. Below, we present a few directions as examples.

5.2.1 Unveiling Hidden Causes of Vulnerability. While prior research provided support for the socio-ecological view, we see the need for future research to delve into the interactions across layers to fully explain the diversity of older adults. Within cybersecurity research, prior work has largely focused on individual factors that contribute to older adults' vulnerability [67], with a few extending to family dynamics [137, 139] and community support [39, 148, 226]. Although other HCI and CSCW studies have looked more broadly into historical changes [17] and explored other sources of support [158], they largely focus on more general technology use.

As a result, the influence of many systems at the outer layers, especially how they together impact older adults' vulnerability, remains largely understudied in the context of cybersecurity. From a socio-ecological view, to study the prevalence of scams targeting older adults [31], future research can look into the interactions among multiple stakeholders in the micro and exo layers — family members, senior care facilities, social workers, store technicians, law enforcement, and more — when combating scams and other digital safety threats directed at older adults.

Additionally, many systems at the outer layers still need exploration, especially considering the constantly evolving landscape of technologies and broader structures. For instance, studying the

impact of emerging dark patterns and deceptive designs at the exo layer on older adults' decision-making and digital well-being could be an important and promising direction [128]. As a way forward, future work can further look into how older adults' S&P, including associated interactions at different layers, might be influenced by factors at the macro layer, ranging from historical trends of technological development, relevant public policies, and societal attitudes toward aging.

5.2.2 Unpacking Vulnerability in Relation to Major Life Events and Broader Changes. The socio-ecological view highlights how vulnerability evolves over time — a critical lens to be considered when studying older adults' S&P vulnerabilities. While the broader HCI and CSCW research acknowledges aging as an ongoing life journey [17, 26, 161], this perspective has been understudied in usable S&P research, leaving many privacy-critical moments and patterns unexplored. For instance, data preparation for death is an extremely relevant theme to older adults [226]; yet, prior work on post-death data preparation has been mostly done with younger [30] or mixed-aged populations [37, 90]. Other major life events related to older adults, such as retirement, bereavement, and changes in living arrangements, could also cause "disruptions" to their digital assets and bear S&P implications [142] while lacking attention in the literature.

Regarding the exo, macro, and temporal layers, the impact of many broader changes over older adults' S&P remains unknown. Prior HCI research has shown that shifts in socioeconomic, cultural, and historical conditions, as well as institutional arrangements, can significantly impact older adults' technology use [17]. For instance, the transition from older to newer technologies at the societal level [184], experienced by everyone throughout their lives, often renders established mental models of technologies outdated [17, 161]. Meanwhile, older adults also actively adopted new technologies due to societal changes. For example, research conducted during the COVID-19 pandemic has shown that older adults adapted their technology use to mitigate social isolation as a result of social distancing orders [81, 163, 186], and these changes may have lasting impacts [184]. However, the temporal pattern of older adults' S&P behavior has remained understudied. Future work could look into how institutional and societal changes impact older adults' cybersecurity, privacy, and digital safety, such as how older adults navigate S&P challenges related to mobile payment systems [87] when these systems become ubiquitous under government-initiated policies [178].

5.2.3 Designing Across Layers. When it comes to design, the socio-ecological view of vulnerability can be a useful ideation tool for researchers and designers to brainstorm where to start addressing older adults' S&P needs. Most designs proposed by prior work have been largely restricted to the individual level. For instance, a large body of HCI and CSCW research has sought to improve the accessibility and usability of technologies relevant to older adults, ranging from wearable sensors [220] to voice assistants [27, 202]. Other research has sought to develop privacy education interventions tailored to older adults [6] or embedding cybersecurity guardians in communities of older adults as a step toward the exo layer level of interventions [148]. However, as Knowles and Hanson noted, without a safety warranty providing foundational trust, older adults might still reject new technologies due to fear of making mistakes [108]. Building on existing work, we see the potential for future designs to enable S&P support for older adults at the infrastructural level, such as by coordinating among multiple stakeholders as well as interrogating and improving relevant policies.

On the other hand, while addressing root causes can be a tempting goal, the socio-ecological view reminds us that enacting changes at the macro layer is often challenging, controversial, and may have unintended consequences, as macro-level structures are often long-established [193]. For example, Havers et al. found that older adults experienced structural barriers, stigma, and disempowerment when reporting cybercrime, as well as a feeling of shame and fear of losing independence due to pervasive, ageist, victim blaming societal attitudes [84]. Developing programs

to address these deeply rooted societal norms would likely be a lengthy and complex process as they are deeply internalized within society [97]. Consequently, researchers and practitioners may have to make hard choices of either adapting to existing structures or challenging those very structures when providing support.

6 Using the Socio-Ecological View in Other Cases

We have shown how the socio-ecological view of vulnerability helps us better understand past literature and inform future research directions regarding older adults in the context of S&P. Below, we present two additional examples to show how our proposed framework can benefit research in other scenarios concerning inclusion.

6.1 Reproductive Privacy in the United States

Reproductive privacy is a growing subfield in HCI, CSCW and S&P devoted to studying user vulnerabilities in the face of potential digital risks, particularly in the context of the U.S. With the overturn of Roe v. Wade — the U.S. court case that included pregnancy termination as a constitutional right — access to reproductive healthcare in the U.S. changed dramatically since 2022 [197]. People seeking reproductive healthcare now face an increased demand for privacy and anonymity, which disproportionately affects historically marginalized groups, such as people of color [164] and those without the financial means to travel for care.

However, privacy and anonymity are at odds with common practices that create a digital footprint of one's pregnancy or pregnancy termination. It is common to digitally track menstruation; search for medical advice online; text or call friends; navigate to a doctor's appointment with a map app; and seek peer support from social media. The risks go beyond hypothetical scenarios: unencrypted social media direct messages — accessed through a subpoena — were used as evidence in court as part of a 2022 case against a woman whose pregnancy terminated in Nebraska [103].

The HCI, CSCW and S&P research communities have recognized vulnerabilities associated with reproductive privacy, yet existing research has focused disproportionately on period-tracking apps, suggesting the need for a more unified understanding of the entire landscape of digital risk in this context. The socio-ecological view can guide researchers towards a more holistic and granular understanding of user vulnerability through a broader landscape of technical risk as follows:

- At the individual level, recent work has explored the use and non-use of period tracking apps [34], political actions [131], and feelings of nihilism [131]. Despite the heavy focus on reproductive technologies, some research has recognized that privacy perceptions extend beyond reproductive technologies, encompassing underexplored areas at exo and macro layers such as healthcare services and media narratives [131].
- At the micro layer, prior work on healthcare (although not necessarily on reproductive health) has already broadly identified communities as a critical support structure during health crises [21]. The Electronic Frontier Foundation specified "a partner, family member, or someone else [one] trust[s]" as potential threats to one's reproductive privacy [71]. However, much of the HCI work on reproduction has been centered around women's experiences in heterosexual relationships, with limited engagement by men and in other sexual contexts [200]. Future work can pay more attention to the interactions and collaborative efforts at the micro layer.
- The exo layer maps to existing work's focus on fertility tracking apps' privacy policies and communications of data practices [127, 188, 189], as well as recommendations to prioritize certain technical designs [117]. Future work could continue exploring the role of technology companies in amplifying or mitigating risks for end users while situating companies' practices in other layers such as media influence for a more critical understanding [131].

- At the macro layer, the overturn of Roe v. Wade, a key government policy, serves as the necessary background for all recent work on reproductive privacy in the U.S. context. Moreover, recent work has started to explore the role of religion in the use of period tracking apps [95]. However, the legal landscape is rapidly changing and requires ongoing investigations.
- At the temporal layer, besides changes at different inner layers, what is critical to reproductive privacy is that pregnancy is a continuously ongoing process that needs stage-based care [79]. However, other than Ibrahim et al. [95], existing research rarely takes a longitudinal perspective. There remains a lot to explore about how people update their threat models in response to their own health changes (such as when becoming pregnant or terminating a pregnancy), changes in apps' data practices, and changes in government policy.

Summary. The socio-ecological perspective on vulnerability offers a broader, more comprehensive view of reproductive privacy (beyond user experiences with period-tracking apps) and can facilitate a unified understanding of reproductive privacy across different populations. As research on reproductive privacy continues to expand at different layers, it is essential for future studies to theorize how laws, as well as broader social norms related to gender, sexuality, and families, shape individuals' reproductive privacy from the outermost societal layers to the most personal inner layers. For instance, gendered norms may influence women's vulnerabilities and behaviors across layers through media, healthcare systems, and intimate relationships.

6.2 Responsible Artificial Intelligence

Responsible artificial intelligence (AI) represents another subarea in HCI and CSCW with a growing interest in inclusion. The deployment of AI systems in high-risk domains has raised concerns regarding their disparate impacts on historically marginalized communities [23]. Research has acknowledged that AI systems have the potential to not only make marginalized groups vulnerable to novel algorithmic harms but also perpetuate and exacerbate existing vulnerabilities [107].

Yet, the definition of who is vulnerable to these AI-enabled harms often suffers from the aforementioned limitation of defining vulnerable groups based on hard-coded demographics [23, 155]. Recently, the literature has seen a shift towards acknowledging how AI systems reflect and perpetuate existing structural inequalities [13, 102, 140], with some proposals to account for temporal dynamics involved in deploying algorithms in contexts marked by injustice [60, 169]. Building on these efforts, the socio-ecological view of vulnerability can help towards a unified understanding of how broader social structures interact with other moving parts of the algorithmic ecosystem to make individuals vulnerable to harm as follows:

- At the individual level, prior work has captured people's perceptions and expectations of AI systems and their harms [126, 190]. Although research suggests that individuals' demographics are not strongly associated with their perceptions of AI-caused harm [10, 208], there is evidence that one's political orientation and experiences with the domain in which AI is deployed impact their opinions about algorithmic systems [78]. The absence of consistent patterns at the individual level, however, suggests that these findings might need to be considered alongside broader contextual factors for a more holistic understanding.
- At the micro layer, research is still often unclear on how user vulnerability may arise from collaborative uses of AI such as with family members, friends, and colleagues. For instance, people may disclose others' information and affect others' vulnerability to AI systems [223]. Furthermore, certain AI applications may present unique concerns for stakeholders at this layer. For instance, AI-powered genetic testing poses a risk where the misuse of genomic data could infringe on the privacy not only of the individual but also of their biological relatives [25].

- At the exo layer, research has acknowledged the role of organizations and institutions in affecting people's use of AI systems. For instance, big tech companies have the power to determine the Responsible AI agenda [73], fueling paternalistic and techno-solutionist approaches to social harms caused by AI [141, 165]. Prior work's focus on this outer layer can also be seen in debates concerning the impact of specific design choices on people's use of AI [43, 100]. Yet, there is still much to explore in terms of creating more effective infrastructural support. For example, developers could be concerned about AI ethics but lack the knowledge and capacity to exert change due to a lack of incentives and support [91]. Future work could explore how to help developers build their collective power to resolve AI-caused harms [216].
- At the macro layer, there is a growing call to understanding structural issues embedded in AI systems [13, 102, 140] and incorporating a policymaking perspective in pushing for responsible AI [172]. Research has identified the ideologies and values shaping AI research, finding that they reflect ideals that perpetuate marginalization [22, 23, 72]. Moving forward, research should continue investigating how these power structures are prevalent across layers and influence user vulnerabilities to AI systems.
- At the temporal layer, a critical concern with AI is the unpredictability of the harms it may cause [9, 92], which often emerge through users' everyday interactions with these systems [177]. This highlights the need for long-term risk assessments. However, there is a notable gap in longitudinal studies that examine both the long-term impacts of deploying AI systems and the consequences of their removal [58]. Additionally, research has emphasized the lack of tools and mechanisms that support users in auditing and understanding AI systems in their everyday use [48].

Summary. The socio-ecological perspective on vulnerability similarly offers a broader, more comprehensive view of people's vulnerabilities when interacting with — and being subjected to — AI systems. While there is a growing call to recognize user diversity and involve relevant stakeholders in AI design [45], the landscape of responsible AI informed by a socio-ecological view is more complex and broader than simply increasing users' participation. Moving forward, researchers must consider dynamics at and across different layers shaping user vulnerabilities — for example, how values embedded in AI design are communicated to the public across layers and how such communications shape public perceptions and reactions.

7 Discussion

We hope that our paper serves as a starting point for the HCI, CSCW, and S&P research communities to build on and move towards a more unified understanding of inclusion from the lens of human vulnerability. We advocate for a critical examination of the term *vulnerable populations* and put forward a socio-ecological lens, intending to guide future research to better define, understand, and design for vulnerability in ways that reflect the concept's complexities. Below, we summarize the key contributions of the socio-ecological lens for studying vulnerability (Section 7.1), outline how this lens informs future work on vulnerability broadly beyond specific cases (Section 7.2), and discuss the politics in naming population vulnerable and how to navigate tensions from institutional requirements (Section 7.3). Finally, we reflect on our work's limitations (Section 7.4) before sharing our concluding remarks (Section 7.5).

7.1 Key Contributions of the Socio-Ecological View of Vulnerability

We summarize the benefits of adopting a socio-ecological view of vulnerability as follows. First, the socio-ecological view has the potential to mitigate the three challenges we identified that

the population-specific approach faces. It allows researchers to move beyond simply associating vulnerability with particular demographics. Instead, it aims to reveal the structures underpinning vulnerability across diverse populations while acknowledging heterogeneity within groups. It encourages considerations of the broader macro-level systems and how vulnerability evolves over time — aspects often overlooked in existing research on vulnerability.

Second, the socio-ecological view can enhance communication among research communities with different focuses on inclusion by positioning vulnerability as a unifying concept that connects human experiences. Although the HCI and CSCW communities have made progress at different layers, communication between these fields can often be limited, such as between empirical HCI and policymaking [222]. Viewing inclusion through the lens of vulnerability opens up opportunities for collaboration, and may allow for the development of common knowledge and design principles for certain layers. When vulnerability is framed solely as a characteristic of specific populations, it may seem like a distant concern; however, the underlying structures of vulnerability are often universal. By uncovering the shared structures behind vulnerability, the socio-ecological view can foster connections based not on acts of kindness, but on our mutual capacity to feel hurt [206].

Lastly, the socio-ecological view of vulnerability can serve as a tool for researchers to be more sensitive to their positionality in interacting with and seeking to advocate for the people they work with. While it is important to interrogate the root causes of vulnerability and advocate for systemic changes, enacting changes at the macro level is practically challenging and might result in unintended consequences. The socio-ecological view nudges researchers to consider the relationality within the entire ecosystem — whether to strategically place their designs within existing structures or advocate for broader structural changes. We discuss this point further below when providing recommendations for future research.

7.2 Recommendations for Future Research on Vulnerability

We present three sets of recommendations for how future research can better study vulnerability and advance inclusion informed by the socio-ecological view, summarized in Table 1.

Goals	Specific Recommendations
Define Vulnerability	• Specify what situations lead to vulnerability when choosing research focus. • Avoid assuming and associating vulnerability with certain populations. • Examine the settings, events, and processes concerning vulnerability.
Understand Vulnerability	• Value localized knowledge and consider methods that enable in-depth and structural analysis, such as ethnography and community-based participatory research. • Explore mechanisms that introduce vulnerability, and how vulnerability evolves over time.
Design for Vulnerability	• Consider how designs are connected to various layers and the larger systemic structures. • Keep relationality in mind — consider how designs may affect interconnected systems and people; consider whether to position the designs within the structures or change the layers themselves.

Table 1. Our recommendations for future work to advance inclusion from a socio-ecological perspective.

7.2.1 Defining What Leads to Vulnerability, Rather Than Who is Vulnerable. We advocate for more focus on what leads to the vulnerability experienced by individuals instead of identifying who is most vulnerable. Developing knowledge around populations as big as older adults could risk being too broad, as individuals within the population may experience different vulnerabilities. While future work involving specific populations should continue, we argue that the research questions themselves should dig deeper into specific settings, events, and processes that are critical to vulnerabilities rather than solely relying on demographic categories such as age, gender, and income level. For example, research could specifically look into how vulnerability emerges and evolves during retirement — through a careful analysis of individuals going through the change with considerations of systems and relationships at play. We believe that focusing on the underlying causes of vulnerability could provide more sustainable solutions. For instance, recognizing trauma as a common emotional state associated with vulnerability, trauma-informed design serves as a useful angle for developing safer technology for all, not just those who have experienced trauma [36].

7.2.2 Understanding the Complexity of Vulnerability. Future research should explore methods to unpack complex mechanisms shaping people's experiences of vulnerability, such as ethnography [53], community-based participatory research [85], and longitudinal analysis [63]. These methods are known to produce thick descriptions of participant experiences and/or unpack complex mechanisms. They are also known for the context specificity and depth associated with how participants interpret and understand their experiences [187]. However, these methods are still underrepresented in user vulnerability research, such as in privacy research with marginalized populations [167].

Meanwhile, we are aware of the epistemological values of identifying common attacks, risks, and harms at scale, especially from the perspective of practitioners working in the fast-paced tech industry who may not always have the bandwidth for deep community engagement efforts. Methods informed by positivist traditions can still work to tackle vulnerability if the focus is on generalizability and reproducibility. However, in pursuit of a more unified understanding, it would be beneficial to combine the detailed analysis offered by interpretive methods [187]. We leave the door open for future research to continue exploring and debating on the use of different genres of methods in relation to the research questions concerning vulnerability.

7.2.3 Designing For What Leads to Vulnerability. When it comes to proposing designs and interventions, the socio-ecological view of vulnerability could guide researchers to think through the where, how, and why aspects when designing for vulnerability. For instance, solely focusing on technical tools, and solutions for individuals might not be enough. A growing body of recent work has started to examine people's experiences in the broader context of social structures, laws, and policies [42, 162, 167, 182], by focusing on the care infrastructure [198, 224] and support circles around people [137, 138, 147]. At times, vulnerability is even seen as a desirable human experience that fosters connection [18, 221]. Building on these ongoing discussions, we encourage a deeper exploration of the structures within which the proposed designs are situated, along with reflection on their motivations, potential consequences, and limitations.

While advocating for more holistic support, the socio-ecological perspective also encourages researchers and practitioners to critically reflect on the ethical implications of any deployed design. As discussed in the case of older adults, individuals, and surrounding systems are interconnected and embedded in broader structures. Changes at each layer could impact others within the same layer as well as other layers and bring unintended consequences. Sometimes, the impact could be universally good. For instance, examining older adults' concerns about data management after death can inform theorizing about vulnerability surrounding death in other contexts, as the topic is relevant not just to older adults but to everyone [37, 90]. Other times, however, interventions can

cause unintended harm. For example, challenging existing structures such as family dynamics and societal ideologies could be controversial and value-sensitive, and often leave the responsibilities and risks to the participants themselves [105, 193]. Sometimes, researchers may have to deal with value dilemmas within and outside of communities [99].

7.3 Reflecting on the Politics of Research with "Vulnerable Populations"

The socio-ecological perspective on vulnerability urges a critical examination of the power dynamics involved in labeling certain populations as vulnerable. Our work intends to provoke a radical reconsideration in future research about whether the population-specific approach is truly the most effective method for promoting inclusion. Employing the term *vulnerable populations* to encompass a large population can often dilute the focus of analysis and hinder the consideration of tailored support. For instance, the roles people take are fluid and multi-faceted; older adults can be recipients of caregiving and caregivers at the same time [139]. Relying on the concept of vulnerable populations in a population-specific sense may restrict how researchers engage with the people they work with and understand their behaviors and practices.

Following the recommendations we made in Section 7.2, we consider a *situation-based approach*. We encourage future research to focus on the situation that drives vulnerability to determine whether using an umbrella term to characterize the populations is necessary, as vulnerability can manifest at various levels. For instance, representation bias in algorithms [171] manifests vulnerability at the population level. By contrast, identity theft manifests vulnerability at the individual level [225]; cooperative cybersecurity management between older adults and their caregivers manifests vulnerability at the interpersonal level [139]. It is also important to acknowledge the universality of being vulnerable as a human experience. This shared understanding has fostered solidarity and amplified the collective power of communities, as seen in the growth of cross-community solidarity such as among LGBTQ+, feminism, disability, and immigration movements [20, 201]. All these vulnerabilities differ and require thoughtful understanding and tailored responses.

Finally, we highlight that the politics in deciding who is vulnerable (or not) extends beyond the execution of research, as research also operates within an ecosystem. For instance, current funding structures often rely on categorizing people into specific groups, such as vulnerable populations, requiring researchers and practitioners to tailor their work to fit the criteria and secure support. Hence, it is important for all stakeholders, including funding agencies, technology companies, and policymakers, to critically examine our roles in shaping the politics surrounding vulnerability and working with people. Is it pragmatically possible to move beyond pre-defined categories and capture the true complexities and diversities of human needs and experiences? We leave this as an open question for future discussions.

7.4 Limitations

Our work has several limitations. First, we did not interrogate the deep reasons why prior HCI, CSCW, and S&P research named certain groups as vulnerable. Oftentimes, the reason remains unclear in the papers we cite. Similar to Bellini et al.'s recent work on research practices involving at-risk users [19], future work can conduct interviews with researchers who engage with *vulnerable populations* to understand the rationales and power dynamics behind the naming.

Second, the socio-ecological view of vulnerability we propose is inevitably shaped by our own positionality and may still be power-laden in application. We propose the framework as a starting point to encourage new perspectives for examining vulnerability and promoting inclusion in research and practice. Our framework should not be taken as a new checklist but as a tool to facilitate theorization and reflection. To put the socio-ecological approach into practice, we emphasize that it

should be advanced through meaningful collaboration with relevant stakeholders instead of fueling helicopter research in which people being studied have no say [4].

Third, we are aware that the presented work is shaped by our own backgrounds in U.S. and European academic systems and draws from articles written in English primarily. We observed that researchers and policymakers in many other countries such as Brazil, China, and Japan use terms equivalent to *vulnerable populations* and similar logic when considering inclusion in research and legal regulations [55, 153, 185]. We encourage future discussions on inclusion and vulnerability in more diverse language contexts and cultural traditions.

7.5 Concluding Remarks

This paper reflects on three key challenges associated with the population-specific approach to advance inclusion in HCI and CSCW research. We advocate for a socio-ecological view of vulnerability based on the ecological systems theory (EST) as a potentially suitable conceptual model to theorize the structures leading to vulnerability. We demonstrate how our framework can lead to explanatory and generative insights when applied to examine older adults, as well as how it can transfer to other contexts such as reproductive privacy in the U.S. and responsible AI. With this socio-ecological view, we suggest future research to expand the scope of vulnerability analysis to settings, events, and processes; value localized knowledge and diversify evaluation criteria; and treat vulnerability as a structural and relational problem. We invite the HCI and CSCW communities to build on our framework and continue the re-conceptualization and empirical investigation into vulnerability to advance inclusion.

Acknowledgments

We thank the anonymous reviewers for their valuable feedback. We are also grateful for the Security and Human Behavior (SHB) Workshop in 2023 that sparked discussions about the initial idea of this research. The research is partially funded by the Max Planck Society and the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA – 390781972.

References

[1] CHI 2024. Retrieved August, 2023. Accessibility and Aging. https://chi2024.acm.org/subcommittees/selecting-a-subcommittee/.

[2] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514.

[3] Alessandro Acquisti and Jens Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE security & privacy* 3, 1 (2005), 26–33.

[4] Fernanda Adame. 2021. Meaningful collaborations can end 'helicopter research'. *Nature* 10 (2021).

[5] The UN Refugee Agency. Retrieved October, 2023. UNHCR-IDC Vulnerability Screening Tool - Identifying and addressing vulnerability: a tool for asylum and migration systems. https://www.unhcr.org/media/unhcr-idc-vulnerability-screening-tool-identifying-and-addressing-vulnerability-tool-asylum.

[6] Heba Aly, Yizhou Liu, Reza Ghaiumy Anaraky, Sushmita Khan, Moses Namara, Kaileigh Angela Byrne, and Bart Knijnenburg. 2024. Tailoring Digital Privacy Education Interventions for Older Adults: A Comparative Study on Modality Preferences and Effectiveness. *Proceedings on Privacy Enhancing Technologies* 1 (2024), 635–656.

[7] Melissa L Anderson, Irene W Leigh, and Vincent J Samar. 2011. Intimate partner violence against Deaf women: A review. *Aggression and Violent Behavior* 16, 3 (2011), 200–206.

[8] McKane Andrus and Sarah Villeneuve. 2022. Demographic-reliant algorithmic fairness: Characterizing the risks of demographic data collection in the pursuit of fairness. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*. 1709–1721.

[9] Callen Anthony, Beth A Bechky, and Anne-Laure Fayard. 2023. "Collaborating" with AI: Taking a system view to explore the future of work. *Organization Science* 34, 5 (2023), 1672–1694.

[10] Theo Araujo, Natali Helberger, Sanne Kruikemeier, and Claes H De Vreese. 2020. In AI we trust? Perceptions about automated decision-making by artificial intelligence. *AI & society* 35, 3 (2020), 611–623.
[11] Rosa I Arriaga. 2017. Using an ecological systems approach to target technology. *Autism Imaging and Devices* 419 (2017).
[12] World Medical Association. Retrieved October, 2023. WMA DECLARATION OF HELSINKI – ETHICAL PRINCIPLES FOR MEDICAL RESEARCH INVOLVING HUMAN SUBJECTS. https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/.
[13] Chelsea Barabas, Colin Doyle, JB Rubinovitz, and Karthik Dinakar. 2020. Studying up: reorienting the study of algorithmic fairness around issues of power. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*. 167–176.
[14] Natã M Barbosa, Jordan Hayes, Smirity Kaushik, and Yang Wang. 2022. "Every Website Is a Puzzle!": Facilitating Access to Common Website Features for People with Visual Impairments. *ACM Transactions on Accessible Computing (TACCESS)* 15, 3 (2022), 1–35.
[15] Jeffery Bardzell. Retrieved August, 2023. A Dark Pattern in Humanistic HCI. https://interactionculture.net/2016/02/03/a-dark-pattern-in-humanistic-hci/.
[16] Shaowen Bardzell. 2010. Feminist HCI: taking stock and outlining an agenda for design. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 1301–1310.
[17] Belén Barros Pena, Rachel E Clarke, Lars Erik Holmquist, and John Vines. 2021. Circumspect users: Older adults as critical adopters and resistors of technology. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–14.
[18] Kristen Barta, Cassidy Pyle, and Nazanin Andalibi. 2023. Toward a Feminist Social Media Vulnerability Taxonomy. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW1 (2023), 1–37.
[19] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L Mazurek, Dana Cuomo, Nicola Dell, and Thomas Ristenpart. 2024. Sok: Safer digital-safety research involving at-risk users. In *IEEE Symposium on Security and Privacy (SP '24)*. IEEE, San Francisco, California, USA, 74:1–74:31.
[20] Patricia Berne, Aurora Levins Morales, David Langstaff, and Sins Invalid. 2018. Ten principles of disability justice. *WSQ: Women's Studies Quarterly* 46, 1 (2018), 227–230.
[21] Karthik S Bhat, Amanda K Hall, Tiffany Kuo, and Neha Kumar. 2023. "We are half-doctors": Family Caregivers as Boundary Actors in Chronic Disease Management. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW1 (2023), 1–29.
[22] Abeba Birhane, Pratyusha Kalluri, Dallas Card, William Agnew, Ravit Dotan, and Michelle Bao. 2022. The values encoded in machine learning research. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*. 173–184.
[23] Abeba Birhane, Elayne Ruane, Thomas Laurent, Matthew S. Brown, Johnathan Flowers, Anthony Ventresque, and Christopher L. Dancy. 2022. The forgotten margins of AI ethics. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*. 948–958.
[24] Lindsay Blackwell, Jean Hardy, Tawfiq Ammari, Tiffany Veinot, Cliff Lampe, and Sarita Schoenebeck. 2016. LGBT parents and social media: Advocacy, privacy, and disclosure during shifting social movements. In *Proceedings of the 2016 CHI conference on human factors in computing systems*. 610–622.
[25] Luca Bonomi, Yingxiang Huang, and Lucila Ohno-Machado. 2020. Privacy challenges and research opportunities for genomic data sharing. *Nature genetics* 52, 7 (2020), 646–654.
[26] Robin Brewer and Anne Marie Piper. 2016. " Tell It Like It Really Is" A Case of Online Content Creation and Sharing Among Older Adult Bloggers. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 5529–5542.
[27] Robin N Brewer, Christina Harrington, and Courtney Heldreth. 2023. Envisioning Equitable Speech Technologies for Black Older Adults. In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*. 379–388.
[28] Robin N Brewer and Anne Marie Piper. 2017. xPress: Rethinking design for aging and accessibility through an IVR blogging system. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–17.
[29] Urie Bronfenbrenner. 2000. *Ecological systems theory*. Oxford University Press.
[30] Jed R Brubaker, Lynn S Dombrowski, Anita M Gilbert, Nafiri Kusumakaulika, and Gillian R Hayes. 2014. Stewarding a legacy: responsibilities and relationships in the management of post-mortem data. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 4157–4166.
[31] David Burnes, Charles R Henderson Jr, Christine Sheppard, Rebecca Zhao, Karl Pillemer, and Mark S Lachs. 2017. Prevalence of financial fraud and scams among older adults in the United States: A systematic review and meta-analysis. *American journal of public health* 107, 8 (2017), e13–e21.
[32] Ryan Calo. 2016. Privacy, vulnerability, and affordance. *DePaul L. Rev.* 66 (2016), 591.

[33] Katie Canales. Retrieved January, 2024. Mark Zuckerberg said he's 'retooling' Facebook toward young adults and away from older users. https://www.businessinsider.com/mark-zuckerberg-facebook-retooling-young-adults-2021-10.
[34] Jiaxun Cao, Hiba Laabadli, Chase H Mathis, Rebecca D Stern, and Pardis Emami-Naeini. 2024. " I Deleted It After the Overturn of Roe v. Wade": Understanding Women's Privacy Concerns Toward Period-Tracking Apps in the Post Roe v. Wade Era. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–22.
[35] Stevie Chancellor, Shion Guha, Jofish Kaye, Jen King, Niloufar Salehi, Sarita Schoenebeck, and Elizabeth Stowell. 2019. The relationships between data, power, and justice in cscw research. In *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing*. 102–105.
[36] Janet X Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. 2022. Trauma-informed computing: Towards safer technology experiences for all. In *Proceedings of the 2022 CHI conference on human factors in computing systems*. 1–20.
[37] Janet X Chen, Francesco Vitale, and Joanna McGrenere. 2021. What Happens After Death? Using a Design Workbook to Understand User Expectations for Preparing Their Data. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–13.
[38] Carl H Coleman. 2009. Vulnerability as a regulatory category in human subject research. *Journal of Law, Medicine & Ethics* 37, 1 (2009), 12–18.
[39] Raymundo Cornejo, Robin Brewer, Caroline Edasis, and Anne Marie Piper. 2016. Vulnerability, sharing, and privacy: Analyzing art therapy for older adults with dementia. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. 1572–1583.
[40] Mayara Costa Figueiredo and Yunan Chen. 2021. Health data in fertility care: an ecological perspective. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–17.
[41] Kimberlé W Crenshaw. 2017. *On intersectionality: Essential writings*. The New Press.
[42] Alaa Daffalla, Lucy Simko, Tadayoshi Kohno, and Alexandru G Bardas. 2021. Defensive technology use by political activists during the Sudanese revolution. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 372–390.
[43] Jenny L Davis. 2023. 'Affordances' for Machine Learning. In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*. 324–332.
[44] Lennard J Davis. 2010. Constructing normalcy. *The disability studies reader* 3 (2010), 3–19.
[45] Fernando Delgado, Stephen Yang, Michael Madaio, and Qian Yang. 2023. The Participatory Turn in AI Design: Theoretical Foundations and the Current State of Practice. In *Proceedings of the 3rd ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization*. 1–23.
[46] Nicola Dell and Neha Kumar. 2016. The ins and outs of HCI for development. In *Proceedings of the 2016 CHI conference on human factors in computing systems*. 2220–2232.
[47] François Delor and Michel Hubert. 2000. Revisiting the concept of 'vulnerability'. *Social science & medicine* 50, 11 (2000), 1557–1570.
[48] Alicia DeVos, Aditi Dhabalia, Hong Shen, Kenneth Holstein, and Motahhare Eslami. 2022. Toward User-Driven Algorithm Auditing: Investigating users' strategies for uncovering harmful algorithmic behavior. In *Proceedings of the 2022 CHI conference on human factors in computing systems*. 1–19.
[49] Mark Diaz. 2019. Algorithmic technologies and underrepresented populations. In *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing*. 47–51.
[50] Cambridge Dictionary. Retrieved October, 2023. vulnerability. https://dictionary.cambridge.org/us/dictionary/english/vulnerability.
[51] Tawanna R Dillahunt, Sheena Erete, Roxana Galusca, Aarti Israni, Denise Nacu, and Phoebe Sengers. 2017. Reflections on design methods for underserved communities. In *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. 409–413.
[52] Lynn Dombrowski, Ellie Harmon, and Sarah Fox. 2016. Social justice-oriented interaction design: Outlining key design strategies and commitments. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*. 656–671.
[53] Paul Dourish. 2014. Reading and interpreting ethnography. In *Ways of Knowing in HCI*. Springer, 1–23.
[54] Bram B Duivenvoorde. 2015. *The consumer benchmarks in the unfair commercial practices directive*. Vol. 5. Springer.
[55] Junko Eba and Kenichi Nakamura. 2022. Overview of the ethical guidelines for medical and biological research involving human subjects in Japan. *Japanese Journal of Clinical Oncology* 52, 6 (2022), 539–544.
[56] United Nations Economic and Social Commission for Western Asia. Retrieved October, 2023. vulnerable groups. https://archive.unescwa.org/vulnerable-groups.
[57] Emory James Edwards, Cella Monet Sum, and Stacy M Branham. 2020. Three tensions between personas and complex disability identities. In *Extended abstracts of the 2020 CHI conference on human factors in computing systems*. 1–9.
[58] Upol Ehsan, Ranjit Singh, Jacob Metcalf, and Mark Riedl. 2022. The algorithmic imprint. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*. 1305–1317.

[59] Michael D Ekstrand, Rezvan Joshaghani, and Hoda Mehrpouyan. 2018. Privacy for all: Ensuring fair and equitable privacy protections. In *Conference on fairness, accountability and transparency*. PMLR, 35–47.
[60] Sina Fazelpour, Zachary C Lipton, and David Danks. 2022. Algorithmic fairness and the situated dynamics of justice. *Canadian Journal of Philosophy* 52, 1 (2022), 44–60.
[61] Isabela Figueira, Yoonha Cha, and Stacy M Branham. 2024. Intersecting Liminality: Acquiring a Smartphone as a Blind or Low Vision Older Adult. In *Proceedings of the 26th International ACM SIGACCESS Conference on Computers and Accessibility*. 1–14.
[62] Martha Albertson Fineman. 2010. The vulnerable subject and the responsive state. *EmoRy lJ* 60 (2010), 251.
[63] Garrett M Fitzmaurice, Nan M Laird, and James H Ware. 2012. *Applied longitudinal analysis*. John Wiley & Sons.
[64] The Organisation for Economic Co-operation and Development. Retrieved October, 2023. Consumer vulnerability in the digital age. https://www.oecd.org/publications/consumer-vulnerability-in-the-digital-age-4d013cc5-en.htm.
[65] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise" How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–13.
[66] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM on human-computer interaction* 1, CSCW (2017), 1–22.
[67] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. 2019. Privacy and security threat models and mitigation strategies of older adults. In *Fifteenth symposium on usable privacy and security (SOUPS 2019)*. 21–40.
[68] Simson Garfinkel and Heather Richter Lipford. 2014. *Usable security: History, themes, and challenges*. Morgan & Claypool Publishers.
[69] Aakash Gautam, Chandani Shrestha, Deborah Tatar, and Steve Harrison. 2018. Social photo-elicitation: The use of communal production of meaning to hear a vulnerable population. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–20.
[70] GDPR. Retrieved October, 2023. Recital 75: Risks to the Rights and Freedoms of Natural Persons. https://gdpr-info.eu/recitals/no-75/.
[71] Gennie Gebhart and Dale Barnett. 2022. *Should You Really Delete Your Period Tracking App?* Retrieved July 4, 2024 from https://www.eff.org/deeplinks/2022/06/should-you-really-delete-your-period-tracking-app
[72] Timnit Gebru and Émile P Torres. 2024. The TESCREAL bundle: Eugenics and the promise of utopia through artificial general intelligence. *First Monday* (2024).
[73] Anne Gerdes. 2022. The tech industry hijacking of the AI ethics research agenda and why we should reclaim it. *Discover Artificial Intelligence* 2, 1 (2022), 25.
[74] H Charles J Godfray. 2002. Challenges for taxonomy. *Nature* 417, 6884 (2002), 17–19.
[75] Bruce G Gordon. 2020. Vulnerability in research: Basic ethical concepts and general approach to review. *Ochsner Journal* 20, 1 (2020), 34–38.
[76] Ellen Gordon-Bouvier. 2019. Relational vulnerability: The legal status of cohabiting carers. *Feminist Legal Studies* 27, 2 (2019), 163–187.
[77] UK Government. Retrieved October, 2023. Syrian Vulnerable Persons Resettlement Scheme (VPRS) Guidance for local authorities and partners. https://assets.publishing.service.gov.uk/media/5a8209abe5274a2e87dc0d21/170711_Syrian_Resettlement_Updated_Fact_Sheet_final.pdf.
[78] Nina Grgić-Hlača, Gabriel Lima, Adrian Weller, and Elissa M Redmiles. 2022. Dimensions of diversity in human perceptions of algorithmic fairness. In *Proceedings of the 2nd ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization*. 1–12.
[79] Xinning Gui, Yu Chen, Yubo Kou, Katie Pine, and Yunan Chen. 2017. Investigating support seeking from peers for pregnancy in online health communities. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–19.
[80] Francisco J Gutierrez and Sergio F Ochoa. 2016. Mom, I do have a family! Attitudes, agreements, and expectations on the interaction with Chilean older adults. In *Proceedings of the 19th ACM conference on computer-supported cooperative work & social computing*. 1402–1411.
[81] Kristen R Haase, Theodore Cosco, Lucy Kervin, Indira Riadi, and Megan E O'Connell. 2021. Older adults' experiences with using technology for socialization during the COVID-19 pandemic: Cross-sectional survey study. *JMIR aging* 4, 2 (2021), e28010.
[82] Eszter Hargittai, Anne Marie Piper, and Meredith Ringel Morris. 2019. From internet access to internet skills: digital inequality among older adults. *Universal Access in the Information Society* 18 (2019), 881–890.
[83] Ayako A Hasegawa, Daisuke Inoue, and Mitsuaki Akiyama. 2024. How WEIRD is Usable Privacy and Security Research?. In *USENIX Security Symposium (SSYM '24)*. USENIX, Philadelphia, Pennsylvania, USA.

[84] Benjamin Havers, Kartikeya Tripathi, Alexandra Burton, Wendy Martin, and Claudia Cooper. 2024. A qualitative study exploring factors preventing older adults from reporting cybercrime and seeking help. *CrimRxiv* (2024).
[85] Gillian R Hayes. 2014. Knowing by doing: action research as an approach to HCI. In *Ways of Knowing in HCI*. Springer, 49–68.
[86] Jordan Hayes, Smirity Kaushik, Charlotte Emily Price, and Yang Wang. 2019. Cooperative privacy and security: Learning from people with visual impairments and their allies. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 1–20.
[87] Changyang He, Lu He, Zhicong Lu, and Bo Li. 2023. "I Have to Use My Son's QR Code to Run the Business": Unpacking Senior Street Vendors' Challenges in Mobile Money Collection in China. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW1 (2023), 1–28.
[88] Franziska Herbert, Steffen Becker, Annalina Buckmann, Marvin Kowalewski, Jonas Hielscher, Yasemin Acar, Markus Dürmuth, Yixin Zou, and M Angela Sasse. 2024. Digital Security—A Question of Perspective. A Large-Scale Telephone Survey with Four At-Risk User Groups. In *IEEE Symposium on Security and Privacy. IEEE, New York, NY, USA*. 1–20.
[89] Kenneth Holstein, Jennifer Wortman Vaughan, Hal Daumé III, Miro Dudik, and Hanna Wallach. 2019. Improving fairness in machine learning systems: What do industry practitioners need?. In *Proceedings of the 2019 CHI conference on human factors in computing systems*. 1–16.
[90] Jack Holt, Jan David Smeddinck, James Nicholson, Vasilis Vlachokyriakos, and Abigail C Durrant. 2024. Post-mortem information management: exploring contextual factors in appropriate personal data access after death. *Human–Computer Interaction* (2024), 1–36.
[91] Jason I Hong. 2023. Teaching the FATE Community about Privacy. *Commun. ACM* 66, 8 (2023), 10–11.
[92] Jason I Hong. Retrieved August, 2023. Why is Privacy So Hard? https://cacm.acm.org/blogs/blog-cacm/235401-why-is-privacy-so-hard/fulltext.
[93] Maarten Houben, Nena van As, Nitin Sawhney, David Unbehaun, and Minha Lee. 2023. Participatory Design for Whom? Designing Conversational User Interfaces for Sensitive Settings and Vulnerable Populations. In *Proceedings of the 5th International Conference on Conversational User Interfaces*. 1–4.
[94] Carrie Hough. Retrieved October, 2023. The UK Government's Approach to Evaluating the Vulnerable Persons and Vulnerable Children's Resettlement Schemes. https://assets.publishing.service.gov.uk/media/5f62301ce90e072bc2c791e6/uk-approach-evaluating-vulnerable-resettlement-schemes-horr106.pdf.
[95] Zaidat Ibrahim, Pallavi Panchpor, Novia Nurain, and James Clawson. 2024. "Islamically, I am no longer on my period": A Study of Menstrual Tracking in Muslim Women in the US. (2024).
[96] Jane Im, Jill Dimond, Melody Berton, Una Lee, Katherine Mustelier, Mark S Ackerman, and Eric Gilbert. 2021. Yes: Affirmative consent as a theoretical framework for understanding and imagining social platforms. In *Proceedings of the 2021 CHI conference on human factors in computing systems*. 1–18.
[97] Loredana Ivan and Stephen J Cutler. 2021. Ageism and technology: the role of internalized stereotypes. *University of Toronto Quarterly* 90, 2 (2021), 127–139.
[98] Pranjal Jain, Rama Adithya Varanasi, and Nicola Dell. 2021. "Who is protecting us? No one!" Vulnerabilities Experienced by Low-Income Indian Merchants Using Digital Payments. In *ACM SIGCAS Conference on Computing and Sustainable Societies*. 261–274.
[99] Rebecca M Jonas and Benjamin V Hanrahan. 2022. Designing for Shared Values: Exploring Ethical Dilemmas of Conducting Values Inclusive Design Research. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–20.
[100] Mackenzie Jorgensen, Hannah Richert, Elizabeth Black, Natalia Criado, and Jose Such. 2023. Not so fair: The impact of presumably fair machine learning models. In *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society*. 297–311.
[101] Eleni Kaprou. 2020. The legal definition of 'vulnerable'consumers in the UCPD: Benefits and limitations of a focus on personal attributes. In *Vulnerable Consumers and the Law*. Routledge, 51–67.
[102] Atoosa Kasirzadeh. 2022. Algorithmic fairness and structural injustice: Insights from feminist political philosophy. In *Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society*. 349–356.
[103] Martin Kaste. 2022. *Nebraska cops used Facebook messages to investigate an alleged illegal abortion.* Retrieved July 4, 2024 from https://www.npr.org/2022/08/12/1117092169/nebraska-cops-used-facebook-messages-to-investigate-an-alleged-illegal-abortion
[104] Smirity Kaushik, Natã M Barbosa, Yaman Yu, Tanusree Sharma, Zachary Kilhoffer, JooYoung Seo, Sauvik Das, and Yang Wang. 2023. {GuardLens}: Supporting Safer Online Browsing for People with Visual Impairments. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. 361–380.
[105] Saba Kawas, Ye Yuan, Akeiylah DeWitt, Qiao Jin, Susanne Kirchner, Abigail Bilger, Ethan Grantham, Julie A Kientz, Andrea Tartaro, and Svetlana Yarosh. 2020. Another decade of IDC research: Examining and reflecting on values and ethics. In *Proceedings of the interaction design and children conference*. 205–215.

[106] Kenneth Kipnis. 2001. Vulnerability in research subjects: A bioethical taxonomy. *Ethical and policy issues in research involving human participants* 2 (2001).

[107] Bran Knowles, Jasmine Fledderjohann, John T Richards, and Kush R Varshney. 2023. Trustworthy AI and the Logics of Intersectional Resistance. In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*. 172–182.

[108] Bran Knowles and Vicki L Hanson. 2018. Older adults' deployment of 'distrust'. *ACM Transactions on Computer-Human Interaction (TOCHI)* 25, 4 (2018), 1–25.

[109] Bran Knowles and Vicki L Hanson. 2018. The wisdom of older technology (non) users. *Commun. ACM* 61, 3 (2018), 72–77.

[110] Bran Knowles, Vicki L Hanson, Yvonne Rogers, Anne Marie Piper, Jenny Waycott, Nigel Davies, Aloha Hufana Ambe, Robin N Brewer, Debaleena Chattopadhyay, Marianne Dee, et al. 2021. The harm in conflating aging with accessibility. *Commun. ACM* 64, 7 (2021), 66–71.

[111] Youjin Kong. 2022. Are "intersectionally fair" ai algorithms really fair to women of color? a philosophical analysis. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*. 485–494.

[112] Jess Kropczynski, Zaina Aljallad, Nathan Jeffrey Elrod, Heather Lipford, and Pamela J Wisniewski. 2021. Towards building community collective efficacy for managing digital privacy and security within older adult communities. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (2021), 1–27.

[113] Priya C Kumar, Marshini Chetty, Tamara L Clegg, and Jessica Vitak. 2019. Privacy and security considerations for digital technology use in elementary schools. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[114] Vilma Lehtinen, Jaana Näsänen, and Risto Sarvas. 2009. "A Little Silly and Empty-Headed"–Older Adults' Understandings of Social Networking Sites. *People and Computers XXIII Celebrating People and Technology* (2009), 45–54.

[115] Carol Levine, Ruth Faden, Christine Grady, Dale Hammerschmidt, Lisa Eckenwiler, and Jeremy Sugarman. 2004. The limitations of "vulnerability" as a protection for human research participants. *The American Journal of Bioethics* 4, 3 (2004), 44–49.

[116] Calvin A Liang, Sean A Munson, and Julie A Kientz. 2021. Embracing four tensions in human-computer interaction research with marginalized people. *ACM Transactions on Computer-Human Interaction (TOCHI)* 28, 2 (2021), 1–47.

[117] Georgianna E Lin, Elizabeth D Mynatt, and Neha Kumar. 2022. Investigating culturally responsive design for menstrual tracking and sharing practices among individuals with minimal sexual education. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–15.

[118] Tian Lin, Daniel E Capecci, Donovan M Ellis, Harold A Rocha, Sandeep Dommaraju, Daniela S Oliveira, and Natalie C Ebner. 2019. Susceptibility to spear-phishing emails: Effects of internet user demographics and email content. *ACM Transactions on Computer-Human Interaction (TOCHI)* 26, 5 (2019), 1–28.

[119] Bruce G Link and Jo C Phelan. 2001. Conceptualizing stigma. *Annual review of Sociology* 27, 1 (2001), 363–385.

[120] Simi Linton. 2017. Reassigning meaning. In *Beginning with Disability*. Routledge, 20–27.

[121] Sebastian Linxen, Christian Sturm, Florian Brühlmann, Vincent Cassau, Klaus Opwis, and Katharina Reinecke. 2021. How weird is CHI?. In *Proceedings of the 2021 chi conference on human factors in computing systems*. 1–14.

[122] Florencia Luna. 2009. Elucidating the concept of vulnerability: Layers not labels. *IJFAB: International Journal of Feminist Approaches to Bioethics* 2, 1 (2009), 121–139.

[123] Florencia Luna. 2019. Identifying and evaluating layers of vulnerability–a way forward. *developing world bioethics* 19, 2 (2019), 86–95.

[124] Florencia Luna and Sheryl Vanderpoel. 2013. Not the usual suspects: addressing layers of vulnerability. *Bioethics* 27, 6 (2013), 325–332.

[125] Juan F Maestre, Elizabeth V Eikey, Mark Warner, Svetlana Yarosh, Jessica Pater, Maia Jacobs, Gabriela Marcu, and Patrick C Shih. 2018. Conducting research with stigmatized populations: Practices, challenges, and lessons learned. In *Companion of the 2018 ACM conference on computer supported cooperative work and social computing*. 385–392.

[126] Hasan Mahmud, AKM Najmul Islam, Syed Ishtiaque Ahmed, and Kari Smolander. 2022. What influences algorithmic decision-making? A systematic literature review on algorithm aversion. *Technological Forecasting and Social Change* 175 (2022), 121390.

[127] Lisa Mekioussa Malki, Ina Kaleva, Dilisha Patel, Mark Warner, and Ruba Abu-Salma. 2024. Exploring Privacy Practices of Female mHealth Apps in a Post-Roe World. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–24.

[128] Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer. 2021. What makes a dark pattern... dark? Design attributes, normative considerations, and measurement methods. In *Proceedings of the 2021 CHI conference on human factors in computing systems*. 1–18.

[129] Laura Mauldin. 2023. On Trauma in Research on Illness, Disability, and Care. In *Crip Authorship*. New York University Press, 131–141.
[130] Allison McDonald. 2022. *Advancing Digital Safety for High-Risk Communities*. Ph. D. Dissertation.
[131] Nora Mcdonald and Nazanin Andalibi. 2023. "I Did Watch 'The Handmaid's Tale'": Threat Modeling Privacy Post-roe in the United States. *ACM Transactions on Computer-Human Interaction* 30, 4 (2023), 1–34.
[132] Nora McDonald, Karla Badillo-Urquiola, Morgan G Ames, Nicola Dell, Elizabeth Keneski, Manya Sleeper, and Pamela J Wisniewski. 2020. Privacy and power: Acknowledging the importance of privacy research and design for vulnerable populations. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–8.
[133] Nora McDonald and Andrea Forte. 2020. The politics of privacy theories: Moving from norms to vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–14.
[134] Nora McDonald, Rachel Greenstadt, and Andrea Forte. 2023. Intersectional thinking about PETs: A study of library privacy. *Proceedings on Privacy Enhancing Technologies* 2 (2023), 480–495.
[135] Bridget Christine McHugh, Pamela J Wisniewski, Mary Beth Rosson, Heng Xu, and John M Carroll. 2017. Most teens bounce back: Using diary methods to examine how quickly teens recover from episodic online risk exposure. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–19.
[136] Tamir Mendel, Debin Gao, David Lo, and Eran Toch. 2021. An Exploratory Study of Social Support Systems to Help Older Adults in Managing Mobile Safety. In *Proceedings of the 23rd International Conference on Mobile Human-Computer Interaction*. 1–13.
[137] Tamir Mendel and Eran Toch. 2019. My mom was getting this popup: Understanding motivations and processes in helping older relatives with mobile security and privacy. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3, 4 (2019), 1–20.
[138] Tamir Mendel and Eran Toch. 2023. Social Support for Mobile Security: Comparing Close Connections and Community Volunteers in a Field Experiment. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–18.
[139] Helena M Mentis, Galina Madjaroff, Aaron Massey, and Zoya Trendafilova. 2020. The illusion of choice in discussing cybersecurity safeguards between older adults with mild cognitive impairment and their caregivers. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), 1–19.
[140] Milagros Miceli, Julian Posada, and Tianling Yang. 2022. Studying up machine learning data: Why talk about bias when we mean power? *Proceedings of the ACM on Human-Computer Interaction* 6, GROUP (2022), 1–14.
[141] Shakir Mohamed, Marie-Therese Png, and William Isaac. 2020. Decolonial AI: Decolonial theory as sociotechnical foresight in artificial intelligence. *Philosophy & Technology* 33 (2020), 659–684.
[142] Benjamin A Morrison, Lynne Coventry, and Pam Briggs. 2020. Technological change in the retirement transition and the implications for cybersecurity vulnerability in older adults. *Frontiers in psychology* 11 (2020), 623.
[143] Benjamin Alan Morrison, James Nicholson, Lynne Coventry, and Pam Briggs. 2023. Recognising diversity in older adults' cybersecurity needs. In *Proceedings of the 2023 ACM Conference on Information Technology for Social Good*. 437–445.
[144] Diane Morrow, Ryan Gibson, and Wendy Moncur. 2023. Understanding online harms and safety of vulnerable groups going through serious life transitions. In *Workshop on Inclusive Privacy and Security*.
[145] Collins Munyendo, Yasemin Acar, and Adam J Aviv. 2023. "In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya. In *2023 IEEE Symposium on Security and Privacy*.
[146] Elizabeth L Murnane, Tara G Walker, Beck Tench, Stephen Voida, and Jaime Snyder. 2018. Personal informatics in interpersonal contexts: towards the design of technology that supports the social ecologies of long-term mental health management. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–27.
[147] Savanthi Murthy, Karthik S Bhat, Sauvik Das, and Neha Kumar. 2021. Individually vulnerable, collectively safe: The security and privacy practices of households with older adults. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–24.
[148] James Nicholson, Ben Morrison, Matt Dixon, Jack Holt, Lynne Coventry, and Jill McGlasson. 2021. Training and Embedding Cybersecurity Guardians in Older Communities.. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–15.
[149] OECD. 2023. Consumer vulnerability in the digital age. 355 (2023). doi:https://doi.org/10.1787/4d013cc5-en
[150] U.S. Department of Health and Human Services. Retrieved November, 2023. Nuremberg Code: Directives for Human Experimentation. https://ori.hhs.gov/content/chapter-3-The-Protection-of-Human-Subjects-nuremberg-code-directives-human-experimentation.
[151] U.S. Department of Health and Human Services. Retrieved October, 2023. Read the Belmont Report. https://www.sigaccess.org/welcome-to-sigaccess/resources/accessible-writing-guide/.

[152] The U.S. Department of Homeland Security. Retrieved December, 2023. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf.

[153] Ministry of Science and Technology of the People's Republic of China. Retrieved December, 2023. UTF8gbsn Guideline on the Ethics Review of Science and Technology Research (Trial Version) ((). https://www.most.gov.cn/xxgk/xinxifenlei/fdzdgknr/fgzc/gfxwj/gfxwj2023/202310/t20231008_188309.html.

[154] Information Commissioner's Office. Retrieved October, 2023. Safeguard and empower the public, particularly vulnerable groups. https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/ico25-strategic-plan/annual-action-plan-october-2022-october-2023/safeguard-and-empower-the-public/.

[155] Anaelia Ovalle, Arjun Subramonian, Vagrant Gautam, Gilbert Gee, and Kai-Wei Chang. 2023. Factoring the Matrix of Domination: A Critical Review and Reimagination of Intersectionality in AI Fairness. *arXiv preprint arXiv:2303.17555* (2023).

[156] Margaret P. Retrieved August, 2023. Kill Your Personas - How persona spectrums champion real user needs. https://www.sigaccess.org/welcome-to-sigaccess/resources/accessible-writing-guide/.

[157] Carol A Padden and Tom L Humphries. 1988. *Deaf in America: Voices from a culture*. Harvard University Press.

[158] Carolyn Pang, Zhiqin Collin Wang, Joanna McGrenere, Rock Leung, Jiamin Dai, and Karyn Moffatt. 2021. Technology adoption and learning preferences for older adults: evolving perceptions, ongoing challenges, and emerging design opportunities. In *Proceedings of the 2021 CHI conference on human factors in computing systems*. 1–13.

[159] James Pierce, Sarah Fox, Nick Merrill, and Richmond Wong. 2018. Differential vulnerabilities and a diversity of tactics: What toolkits teach us about cybersecurity. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–24.

[160] Anthony T Pinter, Jialun Aaron Jiang, Katie Z Gach, Melanie M Sidwell, James E Dykes, and Jed R Brubaker. 2019. "Am I Never Going to Be Free of All This Crap?" Upsetting Encounters with Algorithmically Curated Content About Ex-Partners. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–23.

[161] Anne Marie Piper, Robin Brewer, and Raymundo Cornejo. 2017. Technology learning and use among older adults with late-life vision impairments. *Universal Access in the Information Society* 16, 3 (2017), 699–711.

[162] Elissa M Redmiles, Mia M Bennett, and Tadayoshi Kohno. 2023. Power in Computer Security and Privacy: A Critical Lens. *IEEE Security & Privacy* 21, 2 (2023), 48–52.

[163] Olivia K Richards, Gabriela Marcu, and Robin N Brewer. 2021. Hugs, bible study, and speakeasies: designing for older adults' multimodal connectedness. In *Proceedings of the 2021 ACM Designing Interactive Systems Conference*. 815–831.

[164] Nandita Rose. 2022. *Roe v Wade ruling disproportionately hurts Black women, experts say.* Retrieved July, 2024 from https://www.reuters.com/world/us/roe-v-wade-ruling-disproportionately-hurts-black-women-experts-say-2022-06-27/

[165] Henrik Skaug Sætra. 2023. Introduction: The Promise and Pitfalls of Techno-solutionism. In *Technology and Sustainable Development*. Routledge, 1–9.

[166] Linda Court Salisbury, Gergana Y Nenkov, Simon J Blanchard, Ronald Paul Hill, Alexander L Brown, and Kelly D Martin. 2023. Beyond income: Dynamic consumer Financial Vulnerability. *Journal of Marketing* 87, 5 (2023), 657–678.

[167] Shruti Sannon and Andrea Forte. 2022. Privacy research with marginalized groups: what we know, what's needed, and what's next. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–33.

[168] Devansh Saxena, Karla Badillo-Urquiola, Pamela J Wisniewski, and Shion Guha. 2021. A framework of high-stakes algorithmic decision-making for the public sector developed through a case study of child-welfare. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–41.

[169] Devansh Saxena, Erina Seh-Young Moon, Aryan Chaurasia, Yixin Guan, and Shion Guha. 2023. Rethinking" Risk" in Algorithmic Systems Through A Computational Narrative Analysis of Casenotes in Child-Welfare. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–19.

[170] Morgan Klaus Scheuerman, Jialun Aaron Jiang, Casey Fiesler, and Jed R Brubaker. 2021. A framework of severity for harmful content online. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–33.

[171] Morgan Klaus Scheuerman, Jacob M Paul, and Jed R Brubaker. 2019. How computers see gender: An evaluation of gender classification in commercial facial analysis services. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–33.

[172] Daniel Schiff, Justin Biddle, Jason Borenstein, and Kelly Laas. 2020. What's next for ai ethics, policy, and governance? a global overview. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*. 153–158.

[173] Ari Schlesinger, W Keith Edwards, and Rebecca E Grinter. 2017. Intersectional HCI: Engaging identity through gender, race, and class. In *Proceedings of the 2017 CHI conference on human factors in computing systems*. 5412–5427.

[174] Sarita Schoenebeck and Lindsay Blackwell. 2020. Reimagining social media governance: Harm, accountability, and repair. *Yale JL & Tech.* 23 (2020), 113.

[175] Doris Schroeder and Eugenijus Gefenas. 2009. Vulnerability: too vague and too broad? *Cambridge Quarterly of Healthcare Ethics* 18, 2 (2009), 113–121.

[176] Carol F Scott, Gabriela Marcu, Riana Elyse Anderson, Mark W Newman, and Sarita Schoenebeck. 2023. Trauma-Informed Social Media: Towards Solutions for Reducing and Healing Online Harm. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–20.

[177] Hong Shen, Alicia DeVos, Motahhare Eslami, and Kenneth Holstein. 2021. Everyday algorithm auditing: Understanding the power of everyday users in surfacing harmful algorithmic behaviors. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–29.

[178] Hong Shen, Cori Faklaris, Haojian Jin, Laura Dabbish, and Jason I Hong. 2020. 'I Can't Even Buy Apples If I Don't Use Mobile Pay?' When Mobile Payments Become Infrastructural in China. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), 1–26.

[179] Erica Shusas, Patrick Skeba, Eric PS Baumer, and Andrea Forte. 2023. Accounting for Privacy Pluralism: Lessons and Strategies from Community-Based Privacy Groups. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–12.

[180] SIGACCESS. Retrieved August, 2023. Accessible Writing Guides. https://medium.com/microsoft-design/kill-your-personas-1c332d4908cc.

[181] Lucy Simko. 2022. *Humans and Vulnerability During Times of Change: Computer Security Needs, Practices, Challenges, and Opportunities*. University of Washington.

[182] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. 2018. Computer security and privacy for refugees in the United States. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 409–423.

[183] Lucy Simko, Harshini Sri Ramulu, Tadayoshi Kohno, and Yasemin Acar. 2023. The Use and Non-Use of Technology During Hurricanes. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW2 (2023), 1–54.

[184] Frances Sin, Sophie Berger, Ig-Jae Kim, and Dongwook Yoon. 2021. Digital social interaction in older adults during the COVID-19 pandemic. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–20.

[185] Dirceu Pereira Siqueira and Lorenna Roberta Barbosa Castro. 2017. Minorias e grupos vulneráveis: a questão terminológica como fator preponderante para uma real inclusão social. *Revista direitos sociais e políticas públicas (UNIFAFIBE)* 5, 1 (2017), 105–122.

[186] Andrew Sixsmith, Becky R Horst, Dorina Simeonov, and Alex Mihailidis. 2022. Older people's use of digital technology during the COVID-19 pandemic. *Bulletin of Science, Technology & Society* 42, 1-2 (2022), 19–24.

[187] Robert Soden, Austin Toombs, and Michaelanne Thomas. 2024. Evaluating interpretive research in HCI. *Interactions* 31, 1 (2024), 38–42.

[188] Qiurong Song, Rie Helene Hernandez, Yubo Kou, and Xinning Gui. 2024. "Our Users' Privacy is Paramount to Us": A Discourse Analysis of How Period and Fertility Tracking App Companies Address the Roe v Wade Overturn. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–21.

[189] Qiurong Song, Renkai Ma, Yubo Kou, and Xinning Gui. 2024. Collective Privacy Sensemaking on Social Media about Period and Fertility Tracking post Roe v. Wade. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW1 (2024), 1–35.

[190] Christopher Starke, Janine Baleis, Birte Keller, and Frank Marcinkowski. 2022. Fairness perceptions of algorithmic decision-making: A systematic review of the empirical literature. *Big Data & Society* 9, 2 (2022), 20539517221115189.

[191] Elizabeth Stowell, Mercedes C Lyson, Herman Saksono, Reneé C Wurth, Holly Jimison, Misha Pavel, and Andrea G Parker. 2018. Designing and evaluating mHealth interventions for vulnerable populations: A systematic review. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–17.

[192] Angelika Strohmayer, Rosanna Bellini, and Julia Slupska. 2022. Safety as a grand challenge in pervasive computing: using feminist epistemologies to shift the paradigm from security to safety. *IEEE Pervasive Computing* 21, 3 (2022), 61–69.

[193] Sharifa Sultana, François Guimbretière, Phoebe Sengers, and Nicola Dell. 2018. Design within a patriarchal society: Opportunities and challenges in designing for rural women in bangladesh. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–13.

[194] Xinru Tang, Xianghua Ding, and Zhixuan Zhou. 2023. Towards Equitable Online Participation: A Case of Older Adult Content Creators' Role Transition on Short-form Video Sharing Platforms. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW2 (2023), 1–22.

[195] Xinru Tang, Yuling Sun, Bowen Zhang, Zimi Liu, RAY LC, Zhicong Lu, and Xin Tong. 2022. "I Never Imagined Grandma Could Do So Well with Technology" Evolving Roles of Younger Family Members in Older Adults' Technology Learning and Use. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–29.

[196] Alexandra To, Angela DR Smith, Dilruba Showkat, Adinawa Adjagbodjou, and Christina Harrington. 2023. Flourishing in the Everyday: Moving Beyond Damage-Centered Design in HCI for BIPOC Communities. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference*. 917–933.

[197] Nina Totenberg and Sarah McCammon. 2022. *Supreme Court overturns Roe v. Wade, ending right to abortion upheld for decades.* Retrieved July, 2024 from https://www.npr.org/2022/06/24/1102305878/supreme-court-abortion-roe-v-wade-decision-overturn

[198] Emily Tseng, Mehrnaz Sabet, Rosanna Bellini, Harkiran Kaur Sodhi, Thomas Ristenpart, and Nicola Dell. 2022. Care infrastructures for digital security in intimate partner violence. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–20.

[199] Eve Tuck. 2009. Suspending damage: A letter to communities. *Harvard educational review* 79, 3 (2009), 409–428.

[200] Anupriya Tuli, Azra Ismail, Karthik S Bhat, Pushpendra Singh, and Neha Kumar. 2023. "Information-Backward but Sex-Forward": Navigating Masculinity towards Intimate Wellbeing and Heterosexual Relationships. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–16.

[201] Ethel Tungohan and Fernando Tormos-Aponte. 2023. Social Movements and Intersectional Solidarities. In *The Routledge International Handbook of Intersectionality Studies*. Routledge, 290–303.

[202] Pooja Upadhyay, Sharon Heung, Shiri Azenkot, and Robin N Brewer. 2023. Studying exploration & long-term use of voice assistants by older adults. In *Proceedings of the 2023 CHI conference on human factors in computing systems*. 1–11.

[203] John Vines, Roisin McNaney, Rachel Clarke, Stephen Lindsay, John McCarthy, Steve Howard, Mario Romero, and Jayne Wallace. 2013. Designing for-and with-vulnerable people. In *CHI'13 Extended Abstracts on Human Factors in Computing Systems*. 3231–3234.

[204] Jessica Vitak, Yuting Liao, Mega Subramaniam, and Priya Kumar. 2018. 'I Knew It Was Too Good to Be True" The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. *Proceedings of the ACM on human-computer interaction* 2, CSCW (2018), 1–25.

[205] Lisa Waddington. 2020. Exploring vulnerability in EU law: An analysis of "vulnerability" in EU criminal law and consumer protection law". *European Law Review* 45, 6 (2020), 779–801.

[206] Louise Waite, Gill Valentine, and Hannah Lewis. 2014. Multiply vulnerable populations: Mobilising a politics of compassion from the 'capacity to hurt'. *Social & Cultural Geography* 15, 3 (2014), 313–331.

[207] Ari Ezra Waldman. 2020. Cognitive biases, dark patterns, and the 'privacy paradox'. *Current opinion in psychology* 31 (2020), 105–109.

[208] Ruotong Wang, F Maxwell Harper, and Haiyi Zhu. 2020. Factors influencing perceived fairness in algorithmic decision-making: Algorithm outcomes, development procedures, and individual differences. In *Proceedings of the 2020 CHI conference on human factors in computing systems*. 1–14.

[209] Yang Wang. 2017. The third wave? Inclusive privacy and security. In *Proceedings of the 2017 new security paradigms workshop*. 122–130.

[210] Yang Wang. 2018. Inclusive security and privacy. *IEEE Security & Privacy* 16, 4 (2018), 82–87.

[211] Yang Wang, Huichuan Xia, and Yun Huang. 2016. Examining American and Chinese internet users' contextual privacy preferences of behavioral advertising. In *Proceedings of the 19th ACM conference on computer-supported cooperative work & social computing*. 539–552.

[212] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L Mazurek, Manya Sleeper, and Kurt Thomas. 2022. Sok: A framework for unifying at-risk user research. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2344–2360.

[213] Mark Warner, Andreas Gutmann, M Angela Sasse, and Ann Blandford. 2018. Privacy unraveling around explicit HIV status disclosure fields in the online geosocial hookup app Grindr. *Proceedings of the ACM on human-computer interaction* 2, CSCW (2018), 1–22.

[214] Jenny Waycott, Cosmin Munteanu, Hilary Davis, Anja Thieme, Stacy Branham, Wendy Moncur, Roisin McNaney, and John Vines. 2017. Ethical encounters in HCI: implications for research in sensitive settings. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. 518–525.

[215] Jenny Waycott, Greg Wadley, Stefan Schutt, Arthur Stabolidis, and Reeva Lederman. 2015. The Challenge of Technology Research in Sensitive Settings: Case Studies in'ensitive HCI'. In *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction*. 240–249.

[216] David Gray Widder, Derrick Zhen, Laura Dabbish, and James Herbsleb. 2023. It's about power: What ethical concerns do software engineers have, and what do they (feel they can) do about them?. In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*. 467–479.

[217] Jacob O Wobbrock. 2012. Seven Research Contributions in HCI. *Intelligence* 174, 12-13 (2012), 910–950.

[218] Women Against Abuse. 2024. The Language We Use. https://www.womenagainstabuse.org/education-resources/the-language-we-use.

[219] Marisol Wong-Villacres, Aakash Gautam, Wendy Roldan, Lucy Pei, Jessa Dickinson, Azra Ismail, Betsy DiSalvo, Neha Kumar, Tammy Clegg, Sheena Erete, et al. 2020. From needs to strengths: Operationalizing an assets-based design of technology. In *Conference Companion Publication of the 2020 on Computer Supported Cooperative Work and Social*

Computing. 527–535.

[220] Alan Yusheng Wu and Cosmin Munteanu. 2018. Understanding older users' acceptance of wearable interfaces for sensor-based fall risk assessment. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–13.

[221] Shaomei Wu, Jingjin Li, and Gilly Leshed. 2024. Finding My Voice over Zoom: An Autoethnography of Videoconferencing Experience for a Person Who Stutters. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–16.

[222] Qian Yang, Richmond Y Wong, Steven Jackson, Sabine Junginger, Margaret D Hagan, Thomas Gilbert, and John Zimmerman. 2024. The Future of HCI-Policy Collaboration. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–15.

[223] Zhiping Zhang, Michelle Jia, Hao-Ping Lee, Bingsheng Yao, Sauvik Das, Ada Lerner, Dakuo Wang, and Tianshi Li. 2024. "It's a Fair Game", or Is It? Examining How Users Navigate Disclosure Risks and Benefits When Using LLM-Based Conversational Agents. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–26.

[224] Yixin Zou, Allison McDonald, Julia Narakornpichit, Nicola Dell, Thomas Ristenpart, Kevin Roundy, Florian Schaub, and Acar Tamersoy. 2021. The role of computer security customer support in helping survivors of intimate partner violence. In *30th USENIX security symposium (USENIX Security 21)*. 429–446.

[225] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. 2020. Examining the adoption and abandonment of security, privacy, and identity theft protection practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–15.

[226] Yixin Zou, Kaiwen Sun, Tanisha Afnan, Ruba Abusalma, Robin Brewer, and Florian Schaub. 2024. Cross-Contextual Examination of Older Adults' Privacy Concerns, Behaviors, and Vulnerabilities. *Proceedings on Privacy Enhancing Technologies* (2024).

[227] Nikolina Šajn. Retrieved October, 2023. Vulnerable consumers. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690619/EPRS_BRI(2021)690619_EN.pdf.

Received January 2024; revised July 2024; accepted October 2024