Individually Vulnerable, Collectively Safe: The Security and Privacy Practices of Households with Older Adults

SAVANTHI MURTHY, Georgia Institute of Technology, USA
KARTHIK S. BHAT, Georgia Institute of Technology, USA
SAUVIK DAS, Georgia Institute of Technology, USA
NEHA KUMAR, Georgia Institute of Technology, USA

Older adults are especially vulnerable to online cybersecurity and privacy (SP) threats, such as phishing, ransomware, and targeted misinformation campaigns. Prior work has suggested that this vulnerability may be addressed with the design of social SP interfaces, such that groups of individuals might work together on behalf of one another to manage SP threats collectively. To this end, we present findings from a qualitative inquiry conducted with older adults and members of technology-rich middle-income households in urban India, where technology users have been shown to engage in relatively more social SP practices. Our research examines the collaborative behaviors enacted by different members of the household for protection from SP threats. In particular, we show how self-appointed family technology managers straddle the line between stewardship and paternalism in their efforts to protect older adults' from perceived digital threats. We also offer design implications for supporting collaborative cybersecurity within households based on the insights derived from our analysis.

CCS Concepts: • **Security and privacy → Social aspects of security and privacy**.

Additional Key Words and Phrases: older adults; india; social cybsecurity and privacy; qualitative

ACM Reference Format:
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. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW1, Article 138 (April 2021), 24 pages. https://doi.org/10.1145/3449212

1 INTRODUCTION

Older adults are especially vulnerable to online cybersecurity and privacy (SP) threats, such as phishing, ransomware, and targeted misinformation campaigns [32, 41]. Prior work in the emerging discipline of social cybersecurity suggests that one promising path towards addressing this challenge may be through the design of cooperative and stewarded SP interfaces [9, 11], or systems that support groups of individuals in working together or working on behalf of one another to mitigate an individual's susceptibility to SP threats [61]. Much of this prior work has made broad calls to action and the recommendations thereof are targeted towards a general population [7, 13, 14, 61]. Accordingly, it remains unclear how cooperative and stewarded tools might be designed and

Authors' addresses: Savanthi Murthy, Georgia Institute of Technology, Atlanta, GA, 30308, USA, savanthi@gatech.edu; Karthik S. Bhat, Georgia Institute of Technology, Atlanta, GA, 30308, USA, ksbhat@gatech.edu; Sauvik Das, Georgia Institute of Technology, Atlanta, GA, 30308, USA, sauvik@gatech.edu; Neha Kumar, Georgia Institute of Technology, Atlanta, GA, 30308, USA, neha.kumar@gatech.edu.

2573-0142/2021/4-ART138 $15.00
https://doi.org/10.1145/3449212

implemented, or how such stewardship might be supported, in the context of assisting older populations with identifying and responding to SP threats.

Prior work comparing the privacy attitudes and behaviors of people in the US and India suggests that people in India take a more social approach to SP [10]. There is an opportunity, thus, to study social SP practices in India—especially among older adult populations and the communities in which they are embedded—to gain insights into how we might design cooperative and stewarded tools that help older adults with identifying and responding to SP threats. To that end, our research focuses on understanding how older adults in India approach SP, how they are supported (or not) by other household members, and what insights these behaviors might offer for the design of social cybersecurity systems.

Our work investigates SP behaviors in urban Indian households, foregrounding the practices of and influences acting on older adults, and how these practices and influences result from stewardship and cooperation. We draw attention to how collaborative SP practices shape older adults' digital SP in these households, and the impact of these practices on older adults' digital engagements and overall sense of agency. In doing so, we draw from data collected via semi-structured interviews with 20 participants from eight households in Bangalore and Mysore, cities in South India. These participants included older adults and family members from middle-income households [29], where access to personal smartphones and shared family devices such as iPads was relatively commonplace [24, 31]. Our findings highlight the nature of SP stewardship and control within households, and how stewards impose their threat models—mental models of what comprises a threat to SP that shape how they evaluate and react to these threats—onto older adults who are most vulnerable to security threats.

Our paper contributes a discussion of the roles and organization of SP control within the social groups we studied—of technologically equipped middle-income households in India. In so doing, we advance existing scholarship that examines SP beyond relatively homogeneous western contexts, studying in depth the role of SP as a collaborative practice. In particular, we offer an understanding of the observability of and stewardship around older adults' use of digital technologies in multi-generational households. We investigate the concept of imposed threat models among older adults, and how they influence SP perceptions and practices. Finally, we offer design implications for technology that supports social cybersecurity through pathways of learning, teaching, and translation, in ways that honor the desired agency and independence of older adults.

2 RELATED WORK

2.1 Cybersecurity as a Collective Practice

Prior research on home network management has examined the collaboration and division of labor for *'digital housekeeping'* [18, 44, 45, 49, 56, 58] and found that different household members assumed different roles, such as *'gurus', 'assisters'* and *'consumers'*, where members with technical knowledge were considered experts and typically provided informal technical support [44, 45]. They found that social routines and interactions within households played as important a role as technical resources for digital housekeeping [18, 44, 45], and highlighted the social dynamics that could affect decisions related to technology management, such as how 'gurus' decided if they wanted to provide technical help [45], or the tension between individual and collective management of media, like music [18] or photos[19], within households. This body of work contributed an analysis of the household dynamics around technology usage. We situate our study in urban Indian households with older adults, drawing on these previously identified roles to analyze how different individuals collectively managed SP within the household.

Research on SP has also increasingly emphasized the importance of viewing digital SP as a collaborative endeavor extending beyond the individual [3, 13, 25], and several studies have examined collective SP practices in social media usage, where data is typically co-owned [5, 25, 54, 55, 64]. Das et al. have found that social influence plays a role in enhancing individuals' security sensitivity, i.e. *"the awareness of, motivation to use, and knowledge of how to use security and privacy tools"* [11]. Specifically, they found that more observable security tools and behaviors led to pro-SP behavior change, and that experts felt accountable for the SP of friends and loved ones, leading to stewardship [11]. Chouhan et al.'s work on collective feedback mechanisms for individual privacy shows that people want to leverage the knowledge of trusted friends and family and would like decision-making around SP to be collaborative [7]. As a result, there has been a push for technology which allows for collective SP management [13, 14, 61], and prior work has designed and tested prototypes of collaborative SP tools [7, 54, 55]. However, such technologies are not yet widely available. Our study aims to extend the body of work on collaborative SP by leveraging the already collective nature of SP in the urban Indian context to uncover design opportunities for collaborative and inclusive SP tools of the future.

Within familial units, research finds that people want to exercise oversight over children or older adults' online actions, to know that they are being safe [7]. Mendel et al.'s study found that family members were more willing to help older adults with SP issues compared to other online or offline social groups, and could be more effective in guiding them due to their familiarity with the older adults' preferences [37]. Additionally, SP could be difficult and overwhelming for some people, so they offload these actions to members of the household [13, 14]. However, users generally understand that there are SP threats and willingly provide access to family members for maintenance or management of security settings [14]. Within small social groups, each member is held accountable for the security of shared devices, but many conversations around SP and settings never come up, leading to missed opportunities for stewardship [61]. We further these findings by contextualizing them in a setting where households already manage SP collaboratively, and unpack the dynamics of control, digital literacy, and agency which are important to consider while designing social and collaborative tools for SP management.

2.2 Privacy and Security Practices of Older Adults

Research has found that older adults are more susceptible to cybersecurity attacks as compared to other age groups [15, 32, 40], with older women being particularly vulnerable [17]. Frik et al. found that older adults' lack of security awareness and limited experience with technology have made them more prone to scams and data theft and identified factors such as age-related health issues, living situations, and finances that could affect SP risks of older adults [15]. Nicholson et al.'s study showed that older adults in the UK prioritize sources of SP assistance based on availability rather than expertise and favor media such as TV and radio for SP advice over the internet due to their limited SP literacy, and confidence which could lead to greater vulnerability to cybersecurity attacks [40]. Educational approaches such as training programs, information dissemination through popular media, and digital media literacy instructional interventions have been recommended by several studies to enhance older adults' SP literacy [15, 32, 33, 47, 48]. However, Frik et al. argued that factors which make older adults susceptible to cybersecurity attacks, such as limited awareness, social isolation, limited experience, gender and health issues, also act as barriers to learning about SP and could result in lack of self-efficacy about SP [15]. Older adults in the United States, and non-social-media-using older adults in Canada were found to avoid using apps and services to protect against SP threats [47, 48], whereas older adults in Canada who were social media users limited the information they shared online [47]. Another study identified that older adults actively protected their financial information, but did not value the need to protect personal information or

comprehend the risks of sharing identification information with strangers [8]. A common thread across this literature is the additional vulnerability to SP threats that accompany this demographic, with the focus of interventions on empowering older adults to be more aware of and secure from SP threats.

Literature around ageing in HCI proposes expanding the scope of such conversations, explaining that most conversations focus on *'deficits'* in older adults' skills and cognitive abilities to design technologies for their use [60]. They highlight the importance of viewing ageing as an evolving process, taking into account people's unique lived experiences, and to engage with them throughout the design process. On the topic of SP of older adults, researchers studying technology-mediated caregiving for adults with mild cognitive impairments found that caregivers and care-receivers cooperatively negotiate SP-related decisions, and caregivers frequently decide between giving care-receivers autonomy, and keeping them safe from SP threats [35, 38, 43]. McNeill et al.'s study on privacy of pervasive health-monitoring systems designed for older adults found that such systems could often be 'paternal' and take away the privacy and agency of older adults by assuming that they do not need privacy anymore. They provided design implications to prioritize privacy of older adults and allow them to take an active role in managing their own SP [36]. In our study, we examine the dynamics of the multigenerational households in which older adults are engaging in SP behaviors. We study the situated expectations and behaviors around digital SP, seeking to understand how other individuals in the household influence SP practices of older adults.

2.3 Privacy and Security Across Cultures and Geographies

Inquiries into the global utility of SP tools and settings designed in the Global North have found that these designs are not sufficiently localized to address the needs and technology usage patterns of populations in the Global South [4, 23]. Jack et al. studied the SP implications of insufficient localization of platforms on marginalized groups in Cambodia, and put forth recommendations to design and improve privacy tools with a global audience in mind [23]. Vashistha et al.'s review of SP literature in the Global South identified the key factors that influenced SP perceptions and provided design recommendations for SP tools for this context [59]. Conversations around SP for different types of users, including vulnerable groups, with a focus on looking beyond one-size-fits-all solutions have been gaining momentum [34, 63]. Our study builds on this research by studying SP of older adults from middle-income families in urban India, vulnerable populations in the Global South, to understand their collaborative practices and draw from these findings to inform the broader research around SP, and provide recommendations to design tools for collective SP.

Several studies have compared SP practices across countries and found that cultural differences account significantly for differences in privacy management practices and security behavior [3, 5, 6, 51]. Das et al. typified the behavioral triggers that affect SP practices of people across different nationalities and age groups, and found that social triggers were more likely to cause pro-SP behaviors among Indians than other types of triggers. However, in the United States, proactive triggers were the most effective [10]. Comparative studies on privacy show that Indians, in general, were found to be less aware about topics relating to SP as compared to Americans [6, 26, 30, 42], but expressed higher interpersonal privacy concerns [42]. Kumaraguru et al.'s study found that Indians related privacy to personal space and Americans mostly related privacy to information privacy [30].

Prior research on SP in South Asia have focused on women's experiences and examined the role of culture, gender, socio-economic status, and device-sharing on people's privacy practices [1, 2, 27, 50]. Karusala et al.'s work discusses gendered barriers, such as lower exposure to technology among women, needing permission from male family members, and posting what they consider 'respectable' content, that women would have to work around while representing themselves online

[27]. Work on privacy of shared devices examines how people navigate online and offline norms, such as gender and type of relationship between shared users to maintain individual privacy [2, 50]. Ahmed et al.'s study brought out the cultural association and importance of the act of sharing, which played a role in the privacy practices of shared device users in Bangladesh [1]. Both women and older adults are on the margins of Indian society and are both subject to oversight by their families when it comes to technology usage. Hence, these works provide the foundation for our qualitative study into the nuances of Indian older adults' perceptions and approaches to SP as members of families where it is a collective practice.

3 METHODS

The goal of our research was to investigate SP behaviors in urban Indian households, foregrounding the practices of and influences acting on older adults. The focus on urban India emerged from preliminary findings that conveyed SP behaviors previously understudied in literature on cybersecurity as well as older populations. We began by interviewing older adults from urban middle-income households in Bangalore and Mysore, two large cities in South India, where smartphones as well as other computing devices are routinely used. With smartphone and technology usage seeing a rise in India given the availability of affordable mobile handsets [57] and data plans [21], our study included households with multiple internet-connected devices: some shared, and some personal. Upon discovering the collective nature of the SP behaviors that emerged in our early interviews, we decided to expand our study to also include the perspectives of family members, making the household our unit of analysis instead. We provide details on participant selection, data collection, and data analysis, before clarifying our positionality, and conveying some limitations of our approach.

3.1 Research Participants

We initially sought to interview older adults[1] from middle-income households in Bangalore. For each of these participants, we additionally recruited at least one other member of their household, when our preliminary research suggested that SP practices are collective and significantly influenced by close relations. Our initial set of (6) participants, from 2 households, was recruited via the first author's personal social networks including family and friends. The remaining participants were recruited via snowball sampling [53]. Each household that we recruited from was represented by 2-3 members, with at least one older adult and one adult family member. Overall, we conducted 20 semi-structured interviews—these included 11 older adults and 9 family members, from 8 different households. Participants were 20-81 years old, and more identified as female (70%) than male (30%). All participants were fluent in Kannada, comfortable reading and understanding English, used some form of social media, and owned smartphones. Table 1 presents participant demographics, identifying each household by a letter (A-H), and each interviewed individual in the household by a number. The label 'older adult' was assigned based on age, and the label 'technology manager' was assigned based on interview findings. These classifications are not mutually exclusive; they represent the self-organization within households that we observed in the course of our study.

3.2 Data Collection and Analysis

With Institutional Review Board approval, we began recruiting participants and conducting our interviews. All interviews were conducted via phone, and audio-recorded with informed consent. Participants were informed about the measures taken to keep their data secure, including the anonymization of names, and access to recordings and notes being limited to authors. All interviews

[1]We count individuals over the age of 60 as 'older adults', consistent with widely held Indian norms [46].

Table 1. Our research participants map to eight households. We first recruited older adults, expanding our study to include additional (1-2) immediate family members or close friends. OA refers to older adults, and TM indicates technology managers of the household.

Household	Relationship	Age	Participant ID	N
A	Mother (Older Adult)	78	A1 *(OA)*	3
	Daughter	54	A2 *(TM)*	
	Granddaughter	20	A3	
B	Mother-in-law (Older Adult)	67	B1 *(OA)*	3
	Father-in-Law (Older Adult)	75	B2 *(OA)*	
	Daughter-in-law	40	B3 *(TM)*	
C	Mother-in-law (Older Adult)	68	C1 *(OA)*	2
	Daughter-in-law	40	C2	
D	Father (Older Adult)	62	D1 *(OA)*	2
	Daughter	27	D2 *(TM)*	
E	Mother (Older Adult)	77	E1 *(OA)*	2
	Daughter	47	E2 *(TM)*	
F	Mother (Older Adult)	65	F1 *(OA)*	3
	Father (Older Adult)	75	F2 *(OA)*	
	Son	34	F3 *(TM)*	
G	Mother (Older Adult)	70	G1 *(OA)*	3
	Father (Older Adult)	81	G2 *(OA)*	
	Son	35	G3 *(TM)*	
H	Best Friend (Older Adult)	66	H1 *(OA)*	2
	Best Friend	53	H2	

were conducted one-on-one, even when participants belonged to the same household. The semi-structured interviews were designed to attain a general understanding of existing individual and collective SP perceptions, attitudes, and practices of participants. We asked older adults about their SP practices while using social media, net banking, online shopping, ride-sharing, and food delivery services. Additionally, we inquired about their understanding of privacy, how family dynamics influenced privacy behaviors, and the SP threats considered most potent. Specifically, we asked questions like, "What can happen if someone finds out your password?", "Why has your (family member) asked you to follow this guideline?", or "What do you think can happen if you don't (follow the guideline)?" to understand what they considered threats to SP and actions they took to protect against them. We asked family members of these older adults about their own SP practices, perceptions and definitions of privacy, their understanding of SP threats, and mechanisms they employed to keep other household members safe online. Some of these questions included, "When

was the last time you changed your privacy settings on an app?" and "Have there been instances where you thought about the online safety of your (older adult)?".

Interviews were conducted by the first author in Kannada and English; the first and second authors are fluent Kannada speakers. All data from the interviews was transcribed by the first author and translated to English. The data was then separately open-coded [39] by the first two authors, arriving at codes such as 'unintentional action online', 'privacy between family members', and 'embarrassment associated with SP incident'. Any codes that were dissimilar were discussed after every 5-6 interviews to arrive at a consensus. After all interviews had been coded and codes discussed among all authors, these combined codes were organized and reorganized by the first two authors to identify themes, which were inductively analyzed by the entire team until finalized. Ultimately, we identified three high-level themes that we present in this paper: collaborative SP practices within households, perceived vulnerability of older adults leading to imposed threat models, and the consequences of stewardship and imposed threat models on older adults.

3.3 Limitations

Our data represents collaborative SP practices among technology-rich middle-income families in Bangalore and Mysore, which were multi-generational and comprised of at least one older adult. As is typical for qualitative inquiries such as ours, our findings are not representative of all sections of (Indian) society, but aimed at offering a deeper understanding of previously less understood collective SP behaviors towards orienting more extensive future research. To the best of our knowledge, our research is the first to study SP practices of older adults in India and our findings are an important first step in understanding their relationship with SP.

Not every household we interviewed appeared to have a tech manager; this was a label that emerged from our findings *post hoc*. As the role began to emerge in initial interviews, we drew our attention to it more closely, in taking an iterative approach to interviewing. Further, not all members of all households were available to be interviewed. To better understand household behaviors, we did ask questions about all members, but acknowledge that there may be insights missed from this omission of some members of the household.

3.4 Positionality

All authors are of Indian origin, though now living in the United States. The first and second authors have lived in Bangalore for most of their lives. Two authors have previously conducted field research in India, including in Bangalore and Mysore, particularly around interactions with data, and the use of technology among varied social groups in the urban Indian context. Through this work, we seek to highlight how cultural practices influence SP behaviors in less studied non-Western contexts, and among the less studied vulnerable population of older adults.

4 FINDINGS

In the households studied, we found that SP was managed collectively, with different family members playing different SP roles. We observed some family members taking on the self-assigned roles of *tech managers* for SP in the household, corroborating prior research on digital housekeeping that has labelled such roles as 'helpers' and 'gurus' in the past [44, 45]. Our findings extend this line of work in presenting the collective SP management responsibilities of tech managers and their interactions with others in the household. We found that they acted as SP stewards for their families, in addition to proposing and enforcing SP guidelines upon older adults in the household. Below we describe the perceptions and tensions that arose as a result of such management, and the role played by older adults' pre-established habits and cultural practices in the process.

4.1 Collaborative SP Practices Within Households

We now describe the existing collaborative SP practices we observed among our participants. We found that household members took on different roles in these groups: for example, the families we interviewed had a self-appointed *tech manager* who laid down guidelines for safe technology use at home, and took action to mitigate or prevent SP threats on behalf of others in the household. In turn, older adults tended to have their digital behaviors monitored and their SP stewarded by these tech managers. We also found that within families, individual members were comfortable with looking at and sharing each others' devices, and prioritized collective security over individual privacy at home. However, between families and broader social groups, SP conversations were limited to cautionary tales and personal experiences.

4.1.1 Tech management in the households. The households we studied featured three types of roles that each showcased a different level of SP participation and control. This typically included the (1) tech manager(s), (2) young children and older adults, and (3) older children and other adults in the family. The tech manager's role was generally assumed by one or two household members who considered themselves to be SP experts, relative to other family members. They therefore took on the role of checking on these family members' digital engagements. For example, in regards to managing her in-laws' SP (along with their use of smartphones), B3 *(TM)* as the self-appointed tech manager shared, *"They're very curious about apps. Since I've told them how to use it, I also need to make them aware that there are certain times when they can get into trouble—it may be embarrassing at times or they may get cheated at times."*

Using their knowledge to assist family members, tech managers informed us that they established rules and guidelines for technology usage for everyone in their families. These guidelines were predominantly intended for the older adults and young children in the family, and the devices they used were controlled and regularly monitored by the tech managers. In justifying why they created these guidelines, the tech managers we interviewed expressed a desire to keep their family safe through preventative behaviors. E2 *(TM)* mentioned the rules that she had set for her mother:

> *"Only thing is that they need to be careful of whom they friend [on Facebook]…Second, with unknown peoples not to go [accept friend requests] and [do so] only with known [persons]. And to keep screening once in a while. Keep screening your contacts and details…That's what we basically follow."—E2 (TM)*

B3 *(TM)* further elaborated on the rules that she had set for members of her household to follow, explaining how she *"instructed them (in-laws) clearly not to post anything on Facebook which is personal,"* and expected everyone to log out of social media after they were done using it. We found that as these tech managers took charge of managing the SP needs of their families, their motivations were varied. For example, in some families these were altruistic, with participants expressing that since they were more technologically savvy than their family members, they were in a position to look after others' needs. In others, they stemmed from a desire to avoid embarrassing social situations.

4.1.2 SP knowledge gaps among tech managers. Even though they established guidelines and regularly monitored family members' devices, the tech managers acknowledged gaps in their SP knowledge. For instance, E2 *(TM)* expressed hesitation about teaching SP concepts to her mother, *"Many things are difficult for me to understand, so explaining it to her becomes very challenging."* B3 *(TM)* acknowledged that it was sometimes difficult for her to fix issues because she had to figure out what had happened first, especially when shared devices were involved:

> *"It's a trial and error method even for me. One day my phone just started talking, 'hello, hi', I wasn't able to type anything. Then even I had to Google it from another phone and*

> *switch it off. My daughter (10yo) uses my mother's, father-in-law's and mother-in-law's phones so it can go into any mode anytime."—B3 (TM)*

Participants were thus interested in learning more about SP practices. E2 *(TM)* wondered if there was a forum that she could join to better educate herself about the nuances of SP, and said she would *"like to know more about the dos and don'ts so that [she is] more aware and more careful."*

Even when asked about their approaches to addressing SP breaches on social media, tech managers expressed being under-equipped to respond appropriately. E2 *(TM)* expected legal protections to exist, but was not aware of specifics. C2 was aware that there was a cyber cell, but added, *"I'm not aware of the laws pertaining to it. In case of an incident, right now the only information I have is to approach the cyber cell. So, I'll probably do that."*

Participants did express familiarity around dealing with SP breaches in financial services like credit cards. G3 *(TM)* recounted his friend's experience with a false credit card charge: *"He called up customer care of Citibank because he's gone through their payment gateway. Obviously… it is their responsibility to have it secure. So when his number has got hacked from their platform, it is their responsibility to take care of it for him. FIR (First Information Report) copy was raised and shared with the Citibank guys and they reversed the money within 48 hours."* Despite being cautious and financially aware, tech managers recognized that they could not protect against or counter all attacks, which sometimes led to feelings of frustration and helplessness. F3 *(TM)*, whose mother's ATM credentials had been stolen and used, realized while helping her that his knowledge of the course of action did not successfully translate to correction. He expressed frustration about hidden SP norms that come to light only after there has been an incident, making it very hard to protect against such incidents even when family guidelines were being followed. He said:

> *"The bank manager showed us the footage and the bank basically just told me and my mother that because [we] people have exchanged information, which [they] advise against, there's not much we can do first of all. And that this can't be taken to the police either."—F3 (TM)*

4.1.3 Prioritizing collective security over individual privacy in the household. All participants expressed that there were no threats to digital privacy among family members within the household. Relationships between family members were considered sufficiently open and secure, our findings affirmed. For example, D1 *(OA)*, who shared his Facebook account with his wife, said:

> *"If she (wife) requires anything, she will use my Facebook account. There is not much of a boundary line between us that way. So, what I think is relevant, she also thinks is relevant and what she thinks appropriate, I also think appropriate. So, there's no such confusions any time. She sees my Facebook account and uses my Facebook account to see others' account. But very rarely she posts anything. Sometimes she uploads photos or anything."—D1 (OA)*

Other older adults also did not express a strong desire for individual privacy. In fact, A1's *(OA)* phone was shared with other members of the household. Explaining that this behavior was commonplace, she mentioned she did not object to such usage because *"There aren't any secrets that I have on there, right? So no problems."* This willingness of older adult participants to provide their tech managers complete control over their digital resources was leveraged by the tech managers to provide SP help and advice. In fact, in some families, the tech managers regularly went through their older adults' phones and accounts to check for vulnerabilities. When asked if her mother objected to these checks, E2 *(TM)* said:

> *"She's (mother) pretty cool about it, because she also knows about it. She's okay as long as me or my daughter… It's basically to check that she doesn't land into any trouble*

[unintentionally], that's all… because they don't realize… they would've pressed something [by mistake]. So that is the reason [we check]"—E2 (TM)

Finally, tech managers also expressed that it sometimes became necessary to access older adults' devices, in order to effectively carry out their responsibilities. For example, B3 *(TM)* stated that her in-laws did not have a choice but to show her everything they did since they needed her help, otherwise *"it's not going to work."*

4.1.4 Role of close ties in managing SP. Participants suggested that their extended family, friends, and neighbors would not intentionally send them harmful and misleading information. They were therefore more likely to trust forwards and information shared by these close ties as opposed to those shared by acquaintances or those in websites and articles. For example, C1 *(OA)* mentioned that she did not think that posts she saw on Facebook might contain false information because she did not *"allow any unknown people (to be my Facebook friends), so I get posts only from my friends and my relatives."* Tech managers also echoed this trust in close ties. F3 *(TM)* stated that the likelihood that his parents were exposed to fake messages was low since their WhatsApp communications were limited to close ties.

When tech managers had SP concerns or queries, we found that they reached out to their close ties. Participants also expressed a desire to guide and support these close ties when they needed SP-related assistance. B3 *(TM)*, who enjoyed helping older adults in her apartment building, went out of her way to teach them about apps, set up their accounts, and talk to family members who lived in other countries, to sort out their issues. She had access to most of their accounts as well as passwords, and also taught them about good SP practices when possible. She explained that this stewardship started from noticing older adults in her household having trouble adapting to smartphones, and ventured that older adults from neighboring households approached her because:

"Probably because I don't make fun of them or don't laugh when they ask stupid questions. I feel if I were in a place where technology was a little scary, even I'd be scared to touch something expensive and spoil it. These people are not used to seeing phone or laptop since they were young. They want to gel with the new generation, but they are scared. So, I wanted to help bridge the gap for them to connect with whoever they wanted."—B3 *(TM)*

Conversations between tech experts of different families were limited to information about SP breaches that they have faced. This is similar to findings from previous studies, where people felt obliged to share cautionary tales with friends, and others under their care, to prevent them from falling victim to similar attacks [10–12]. We found that conversations regarding SP between groups did not typically focus on security tools or settings, but only around past experiences. However, within households, all aspects of SP—tools, settings, incidents—were discussed and addressed. For example, C2's friend told her about being scammed through a QR code payment request and how this had influenced her own SP behavior:

"She [had] posted an ad for selling a few items. And the person called saying that 'I'm interested in taking your item and I'll pay you this much… as an advance, I'll pay you this much.' And he sent some PayTM request. She thinks it is [a request] to accept money, but then it happened to be the other way around. She has approached [the authorities] and lodged a complaint but they have not been able to find the person. See, even if something like that has come to me, you know, I might pay it without thinking. But, once I know about it, I try to be cautious with it."—C2

We found that SP tools, settings, and guidelines were not shared across different families or households, and were chosen solely based on the knowledge of the tech manager(s) of each family. Hence, the SP of families could be only as strong as the SP of their tech managers.

In sum, we found that 1-2 household members acted as *technology managers* and assisted the older adults in their households by establishing SP guidelines for them, corroborating prior research on caregiving [20] and digital housekeeping [44, 45]. They had varied motivations and attitudes, and varying levels of expertise, but they assumed this role nevertheless. These tech managers were the most knowledgeable about SP within the household, but acknowledged that their SP expertise was limited. They usually looked online or reached out to close ties in their larger communities when they required assistance themselves. SP conversations between different families, however, revolved mainly around cautionary stories based on past experiences and did not extend to specific SP practices, tools, or settings.

4.2 Perceived vulnerability leading to imposed threat models

Family tech managers laid out SP guidelines and regularly monitored older adults' devices to prevent SP lapses because they found older adults to be more vulnerable to SP threats compared to other family members. Additionally, tech managers expressed a sense of responsibility to keep older adults safe from SP threats, and to prevent embarrassment (to either party) caused by unintended actions online. This responsibility, combined with the perceived vulnerability of older adults to SP threats, motivated tech managers to take a somewhat heavy-handed approach: they would manage and even control older adults' actions on their smartphones as a way to protect them against the threat models the tech managers held. In other words, tech managers required older adults to adhere to guidelines meant to defend against an *imposed threat model*—often one which did not align with older adults' conceptions of SP threat. As a result, older adults often did not comprehend these imposed threat models and occasionally ignored the tech managers' SP guidelines in favor of convenience and entertainment. Several tech managers acknowledged that their heavy-handed approach could lead to loss of agency for the older adults, but they could not think of ways to keep older adults' safe.

4.2.1 Motivations for managing. We uncovered three motivations for why our tech manager participants took charge of older adults's SP concerns: (1) the perception that older adults were especially vulnerable to SP threats, (2) a sense of responsibility for the digital wellbeing of older adults, and (3) the desire to prevent embarrassment. We cover each of these below.

Tech managers suggested that it was difficult for older adults to completely understand SP, which made them more vulnerable to SP threats. G3 *(TM)* explained that their extra vulnerability to SP threats stems from their *"ignorance, and to some extent negligence,"* suggesting that a lack of awareness of the consequences of their actions exacerbated this problem:

> *"The problem is, older folks, they're not kind of aware. Because, they've not been, I mean, since we work in IT companies and tech companies, so we know the consequences. We're kind of aware because we write code for it. So, apparently the older generation, they're not aware as to what can happen. So, I would say ignorance and to some extent negligence. So ignorance and negligence, I would say these two words. For the older generation. The older generation is kind of more vulnerable to the security threats."—G3 (TM)*

Additionally, tech managers sometimes found it easier to assume that older adults would have difficulty in understanding SP features on digital services, so they would omit the complexities when explaining SP guidelines associated with these services, and sometimes use these services on behalf of the older adults, as needed. E2 *(TM)* mentioned that she did not want to confuse her mother, and thus chose not to correct her simplifying assumptions around online money transfers:

> *"The other day I was trying to do something through Google pay.[...] She said, 'What's the issue? I have money, I'll give it'. I said,'I have money too. It's not about that.' But sometimes that concept becomes very difficult [to explain]. They know money transfer, they know all*

that. But sometimes for few things, best is to not complicate and not tell them much. In their mind, the transaction is very simple. So best is to keep it simple."—E2 (TM)

There were also occasions where the tech managers referred to older adults as children. For example, E2 *(TM)* said:

"They (older adults) believe [the information they receive online], so I keep telling my mother that it's not authentic what you see or hear in YouTube, but it's very difficult for them to understand that at that age. Because they're like infants who are put into something new. So, I keep telling, I try to do my best, but then can't help beyond a point."—E2 (TM)

They would also enroll their children into the exercise of monitoring their parents' SP practices. For example, E2's 16-year-old daughter helped her manage E2's mother's accounts and was given more freedom on her smartphone, *"So my (16 year-old) daughter's email ID was given (for my mother's Facebook account). We had not created her (mother) own email ID. So that is how we got to know that something like this has happened. So, somebody had accepted her friend request and that's when my daughter told, and we went and checked. So, these things happen, which is little difficult. They understand. But sometimes certain things happen without their knowledge."*

Interviews also brought attention to the need for more SP stewardship within some households. A3 explained that she was aware of A1's *(OA)* embarrassing incidents on Facebook, but *"actually [did not] know if she has any privacy settings."*. D2 *(TM)* could not recall the last time she audited D1's privacy settings on various platforms:

"I really, really don't think so (that they changed privacy settings). My dad has accounts on everything. I think his Facebook thing, after a while he did change it, because I remember asking him about it.... But my mom isn't on anything else except WhatsApp, so I'm pretty sure her privacy settings are open to all. I feel like I saw it and I changed it once. That's why I remember..."—D2 (TM)

Many tech managers expressed that they felt responsible for ensuring the safety of older adults in their households. A2 *(TM)* explained her reason for managing her mother's technology use:

"The older adults don't really know all this, but they want to use the media. They like it, they're enamored by it, so I don't want to deny that. So if she wants to use it, I think we should take the responsibility of keeping her safe also. There's no point in restricting her from using it."—A2 (TM)

Similar findings related to feeling obligated to share SP information and be responsible for the SP behaviors of others have been discussed in prior work [10–12]. Our findings show that tech managers in Indian families who managed SP of older adults not only regularly shared information about SP and set guidelines to ensure collective SP, but also acted on older adults' behalf to minimize risk exposure.

Finally, being able to prevent personal embarrassment was another source of motivation for tech managers to monitor older adults' actions on social media, and even set controls on their behalf without explaining these to them or teaching them how to adjust them. For example, G3 *(TM)* found his father's unintentional actions on Facebook embarrassing and decided to change his privacy settings:

"The problem is, he (father) doesn't know to use [Facebook]... sometimes he uses Facebook from his mobile. He'll go to some profile and he shares it on his wall. Accidentally of course, he doesn't know. And accidentally he sends a friend request to someone... he just clicks somewhere and he does something... He always says he hasn't done it, but he has done it. That is kind of embarrassing... [So] I have put a setting saying that 'What I do should be

seen by me, not by others'…And it's impossible! He can't go and change back the settings if he wanted to (laughs). So, he's free to do anything now."—G3 (TM)

4.2.2 Imposing threat models and controlling behavior. We saw that family tech managers operated and controlled older adults' devices and settings on their behalf to enhance their SP. Decisions were made based on the tech manager's own SP perceptions and threat models and were not often explained to the older adult, like when G3 changed his father's privacy settings as we presented in the previous section. As a result, the family tech manager's threat model was imposed on the older adult, but the logic and rationale that went into developing such threat models were not communicated. When this occurred, family tech managers acknowledged that the older adults might not be able to change these settings back if they wanted to, but justified their actions by arguing that these steps would ensure the safety of the older adults in their charge. This also enabled them to track when the older adults wanted to change these settings because they would have to come back to them for help. F3 *(TM)* said that he had blocked calls from unknown numbers on his parents' phones for their safety:

"On their (parents') phone, what I've done is, I've blocked any calls from any unknown numbers. They have to have the numbers stored into their contacts and only then they can receive such calls. They know about this, but I'm not sure they're very much savvy enough to change the settings by themselves, but they'd surely take my help in doing it."—F3 (TM)

These controls adopted by family members have negatively impacted the agency of older adults and changed the way they interact with digital services. B3 *(TM)* recounted her experience trying to explain how Google Pay works to older adults in her household, from setting up internet banking on their accounts, to digital money transfer. Ultimately when educating turned out to be difficult, she decided to mediate their usage:

"So this [concept] of whatever the software is doing is difficult to take in for them. It will take time. So I have made an arrangement now. I do the transaction and I collect cash. I've told them that unless they ask me, they can't do any of those things. They can't transact, or do anything."—B3 (TM)

We found that this approach hampered the development of a complete threat model among the older adults, and such an imposed threat model resulted in ill-defined fears regarding certain technologies. Financial technologies were readily eschewed, we found, because the consequences of SP breaches were better understood, even if better SP behaviors could not be developed. B3 *(TM)* compared SP behaviors between financial technology and social media in her house:

"When they see the word bank, ATM, password [etc.] they get too scared about it. They don't operate it at all. They'll just ask me what it is. But, when there are friend requests from people on Facebook, they will go ahead and [accept] it. [Only] then, they'll think about if it's a friend or not a friend… why they sent it to me, such kind of questions."—B3 (TM)

Similarly, G3 *(TM)* noted how the older adults in his household stored multiple passwords and other sensitive information, such as universal identifiers, on a cloud-based note-taking software, and the resulting conversations around the trade-off between SP threats and convenience. Although G3 stressed on the SP ramifications of such a system, G2 *(OA)* explained the convenience it introduced. G3 explained the compromise they arrived at as:

"So then I told him, at least…put a password to your phone and do that. That's the bare minimum! Mobile phone is something he carries [all the time] and he didn't even have a homescreen lock. So if your phone gets lost or something, they'll get to know, if they open Evernote or something, they get to know the entire details that are there—his pan card

> *number, Aadhar card number (universal identifiers), bank account number and whatnot, he has everything, all the passwords stored."—G3 (TM)*

Over time, G3 explained to his father (G2) the dangers of having such unprotected content on his mobile phone. We found that despite these warnings, G2 prioritized convenience over security, albeit furtively. G2 said:

> *"Sometimes I forget the password. There are so many passwords. Like bank ATM password, Amazon Prime password etc. For my age it is difficult to remember all passwords. So I note it down in 'Evernote'. But my boys tell me not to type and keep it as someone may get to see it. So, they ask me to memorize it. (But even now) I have kept in Evernote."—G2 (OA)*

Some older adults prioritized entertainment over their family's SP guidelines, since they were not aware of the rationale behind being asked to avoid certain content. E1 *(OA)* said that she did not let these rules come between her and the interesting content that she enjoyed watching:

> *"As I said, I see the horoscope and some useless news that will be coming on (YouTube). I see that. My people say that all those are false and useless, why do you see. But it is very interesting. So, I see. That is all."—E1 (OA)*

These imposed threat models also extended to the smartphone apps that older adults used. B3 *(TM)* mentioned that her in-laws downloaded potentially dangerous apps by mistake. As a result, she regularly screened their phones for apps which appeared harmful or complicated to her.

> *"They don't miss it, they're not aware at all. It would've come as an advertisement on a Youtube video they watched or a forward on WhatsApp or something. So without their knowledge, their fingers would've moved and pressed it and it would've gone and sat on one of the icons."—B3 (TM)*

These impositions restricted the way older adults could interact with digital services, sometimes to their frustration. For example, in the context of social media, older adults expressed that they were not able to control how they represented themselves because their family restricted their use of social media. E1 *(OA)* lamented, *"They (daughter and granddaughter) have put some ugly one (her FB profile picture). They have done it themselves. I would never ask for it. Neither I asked for it nor did I choose the photo. It is quite awful. I want to get it removed. If I want to change it, I will have to tell my granddaughter and she will do it."*

In E1 *(OA)*'s case, the loss of agency was clear since her profile image existed as a part of a service with which she regularly interacted. However, in the scenarios where less frequently used features of technologies were manipulated for better SP, the older adults were not always aware that their online presence was being managed.

4.2.3 Balancing SP and sense of agency. We discussed how tech managers controlled and operated older adults' accounts and settings, imposing their threat models often without explanation. This type of management, in turn, caused older adults to fear using certain services, and reduced their agency over their accounts and actions. Additionally, we found that family tech managers were aware that their impositions and guidelines reduced older adults' agency, but rationalized this loss of agency as being preferable to becoming a victim of an SP incident. A2 *(TM)* stated that her mother was scared that something would happen to her device if she did not follow guidelines:

> *"After telling her so many things, she's getting scared. She's gone to the extent of thinking that if she does something that she's not supposed to do, the phone may even explode. She even goes to that extent. I think all our telling has impaired her freedom with the use of phones and technology that she uses. But I think it's a good thing that she's so scared, because otherwise she can get into trouble."—A2 (TM)*

E2 *(TM)*, on the other hand, mentioned that her mother exercised healthy skepticism while using social media when E2 was around, but was not sure if her mother followed SP guidelines when nobody was watching. Other older adults agreed that household SP guidelines have made them stop using so many features that they might have liked to try out otherwise. They also refrained from interacting on social media due to fear and confusion. A1 *(OA)* said about how the rules have changed her behavior:

> *"(They say) Be careful, don't send everyone a friend request, don't accept everyone's friend request. Everyday I still see these things on my phone screen. I didn't know earlier, I used to press all that. Now I've been told that I'll be charged [money] if I press all that, so I don't press anything. It used to ask, 'later or now'. Now I say later and leave it. Earlier, I used to press the 'yes' (or 'now') for everything."—A1 (OA)*

Such hands-on approaches to SP management at the household level did not directly translate to situations where stewardship was provided for different households. B3 *(TM)*, who helped her older neighbors with technology issues, made a personal choice to maintain her distance and give her neighbors as much control as possible. She noted that she had access to all their accounts but made a decision to support their independence:

> *"I have a personal relationship with them and I also maintain that distance with regard to whatever information I have access to. So I don't talk about it. That's a personal decision because it's not only mother and father-in-law whose phone I look into. I also into other's, neighbor's phones, people whom I know, they have a lot of questions. So I have all their passwords, I have their data with me. So personally, I maintain that distance so that I don't talk about it with anybody else or with them. They actually have no knowledge about what I have access to."—B3 (TM)*

In this section, we discussed the oversight of older adults' actions on digital platforms by tech managers who felt a sense of responsibility to protect them from SP threats, considered them to be more vulnerable to SP threats compared to other family members, and more likely to cause embarrassing incidents. These perceptions and practices led to family tech managers imposing their threat models on older adults, sometimes without explaining the reasons behind certain actions. While this reduced older adults' control over their digital footprint, their tech managers expressed that they are safer because of it, and struggled with finding a balance between keeping them safe and giving them freedom to explore. Older adults, on the other hand, tended to ignore the imposed guidelines when no one was watching, prioritizing convenience and entertainment over SP. Next we examine the impact of these imposed threat models on older adults' SP practices and digital literacy.

4.3 Consequences of tech management and imposed threat models

Older adult participants were generally grateful for help from tech managers. However, we also identified three downstream consequences of tech managers imposing guidelines and controlling older adults' accounts and SP settings. First, older adult participants did not appear to be informed of the extent of their digital footprint—the records of their digital activity as collected by their internet service providers as well as the services and apps they used [62]. Second, they were often unexposed and therefore unaware of the consequences of security breaches. Third, they found it challenging and sometimes unnecessary to learn more about SP or technology, limiting growth in their digital and SP literacies.

4.3.1 Limited information on digital footprints. We found that older adults frequently found it challenging to remember the details of their digital activities. Many older adult participants had

trouble remembering the names and functions of the apps that they used. For example, F2 *(OA)* said, *"How do I record (from YouTube)?...I have an app like something called monkey, jumper monkey. I use that to record."* It turned out that they in fact had no such app installed. Such confusions seemed commonplace, and older adults were generally uninformed about the extent of their online activities and digital footprints. Some older adults were unaware that they had email accounts that were created and completely controlled by their tech managers. These email accounts were used as a means to sign up for third-party services such as Facebook or YouTube. When we asked A1 *(OA)* about the account she used for Facebook and YouTube, she said: *"I don't know all that (if I have an account, if I'm logged in). I just use it all together. I don't know much about all these things, my son takes care of them."—A1 (OA).* G3 *(TM)* echoed this sentiment when he spoke about how his mother uses YouTube through a Gmail account that he and his brother created for her:

> *"She has a Gmail account and she is logged in through Gmail. YouTube, it is already logged in. She just opens YouTube and searches for some video that she likes. Regarding Gmail, she does nothing. I'm sure that she doesn't even remember it (that she has a Gmail account). It's always logged in and she uses it, that's all."—G3 (TM)*

We also found that older adults equated uninstalling an app or removing credit card details from a service with deleting an account and all related data. F2 *(OA)*, who has learnt to use apps from his son, recalled an instance when he had subscribed to a journal online, and provided his credit card information in the process. When he discovered he was being charged for it monthly, he said he had 'cancelled' the service by removing his financial details:

> *"When I was going through my account statements I came to know [I was being charged]. No [I didn't contact the service], I just cancelled it since the amounts were not very big...So I stopped it, I removed my credit card details from that. That is the end of it."—F2 (OA)*

In this way, by acting as hands-on SP stewards for older adults, well-meaning family members may have unwittingly prevented older adults from gaining a comprehensive understanding of their digital footprints. Because they were never keyed into how their digital accounts were created and maintained, many of the older adults we interviewed were unaware of how much of their data and what type of data was online and were also unaware of how to remove their data from a service.

4.3.2 Little knowledge of the consequences of SP breaches. A second side-effect of stewardship and imposed threat models was that our older adult participants had little knowledge regarding the consequences of SP threats and breaches. They followed their tech managers' SP guidelines without fully understanding why, and often had misconceptions when pressed to speculate as to the rationale for the guidelines they had followed. E1 *(OA)* could not explain, for example, as to why her daughter had asked her not to connect with strangers from other countries on Facebook. However, she speculated on the consequence of having an unknown friend on Facebook from another country as follows:

> *"My granddaughter has taught me to be very careful and I follow her instruction. I was told that if such confusions happen, any news or information can go from anywhere to anywhere. It could go out of our country to any other country also. But I really do not know about [what could happen if information goes out of the country]. But if some types of information leak out, it may even harm our nation."—E1 (OA)*

A1 *(OA)*, on the other hand, was sympathetic towards the unknown people who tried to connect with her on social media. She mentioned that the consequence of sending a friend request to an unknown person would be that the friend would send messages without knowing that she is old, and would be disappointed and stop when they found out. She also felt bad that she would not be

able to converse with this person as someone their age would, or as this unknown person might have expected:

> *"If I send it (friend request) to an unknown person, they'll start sending me those types of messages, right? They don't even know me. After they see me, can see my profile picture (and see that I look old), they also become careful. Otherwise they send all sorts of things. That's why (I've learned now that) it's better to be careful."—A1 (OA)*

For G2 *(OA)*, it was difficult to comprehend the impact of his digital SP being violated. He said that his sons ask him to keep his passwords safe at home, but he found it difficult to think of what someone might do with such data:

> *"Nothing will happen [if someone finds out my password]. I won't get privacy, but I have nothing [to protect]. I do not keep any documents or important things. People who keep such things keep their passwords safely. [My sons] tell me not to reveal my password… to others. If someone finds it, they can access my messages on my laptop, but what they will do is just see some bank statements etc. which will be there. They cannot do anything with that."—G2 (OA)*

We found that it was a common practice for SP incidents to be avoided as topics of conversation among the older adults we interviewed. Older adults valued their standing in society and wanted to avoid any changes in the way they would be perceived by their community members if they fell victim to such incidents. For some older adults, this type of embarrassment or change in social status was considered a consequence of a SP breach. For example, D1 *(OA)* did not expect to know about SP incidents faced by his friends:

> *"People normally won't come out and say that they've been cheated or anything, you know, normally they don't say, so I don't know (anyone who had a SP incident) in my close circuit."—D1 (OA)*

Similarly, F3 *(TM)* spoke about his mother (F1 *(OA)*) as having been a victim of an incident at the ATM, but F1 *(OA)* herself never mentioned the incident when she was asked about such experiences during her interview.

4.3.3 Resistance to learning more about SP. The third downstream consequence of stewardship and imposed threat models we found was that older adults considered it difficult and unnecessary to learn more about SP, or technologies in general. They cited age as a barrier to learning more about SP. C1 *(OA)* stated that it was interesting to read about such topics, but that there was no need for people her age to remember or implement them. Additionally, older adults did not see the need to worry about SP because their stewards, in imposing threat models and guidelines to curb those threats, led them to believe that those incidents would not happen to them. Similar beliefs have been uncovered by a prior study that examined the psychology of the home internet user [22]. For example, D1 *(OA)* said that he would not do anything for his own SP based on a threat that someone he knew faced:

> *"I really see whether it (another person's SP incident) is really affecting me first.… Or does it encroach into my privacy or anything. And if it is not, then I ignore the whole issue. I don't bother much about it. See, all this gives way for fear psychosis. So, I try to be ignorant about it."—D1 (OA)*

A prior study by Gaw et al. also found that taking SP actions for information that was not considered sensitive was associated with paranoia [16].

Another reason for older adults to avoid learning about SP was their belief that extensive background knowledge about technology would be necessary to understand SP. G2 *(OA)* mentioned

that he depends on his sons for SP support, saying *"both my sons are in the software line. I am a mechanical fellow. I don't know much about this."*

We noted, as a further example of how imposed threat models engender a false sense of security, that tech managers' attempts at teaching older adults SP practices were sometimes met with resistance. The most common reason that older adults cited for believing that SP was unnecessary for them to learn was that their family members were always around to take care of it on their behalf. A1 *(OA)*, for example, suggested, *"If someone is there (to do online payments and banking on my behalf), I don't need to learn it. Ignorance is best."* We found that such dependence was not just restricted to SP concerns, but also impacted usage of a broader range of technologies. E1 *(OA)* said: *"Yes, they want to teach me how to use Big Basket (grocery store), Ola cabs etc. as I am alone many times and it is useful. But I always have someone do it for me and I don't see the necessity."*

To summarize, our findings demonstrate that SP was considered a family effort in urban Indian families, with self-appointed tech managers within families taking on stewardship roles, and establishing guidelines for tech usage for the whole family. This led to multiple roles for SP control in these groups, with tech managers exerting control over older adults' use of technology even though they may have had gaps in their own SP knowledge. Tech managers expressed that older adults were especially vulnerable to data breaches, and sometimes took a heavy-handed approach to stewardship—controlling their accounts and settings—leading to reduced freedom and agency for the older adults. As a result, tech managers' threat models were imposed on older adults without the older adults understanding the rationale behind SP guidelines or the need for SP. Thus, older adults were left unaware about their own digital footprints and the consequences of SP threats and violations. Such heavy-handed stewardship and imposed threat models exacerbated older adults' resistance towards learning about SP since they found it to be difficult, unnecessary, and already handled by others.

5 DISCUSSION

Our findings demonstrated that enacting SP entails cooperative work in urban Indian households, where tech managers provide and enforce guidelines for other family members, particularly older adults. We learned that the tech managers are not always experts; however, it is not absolute but relative expertise that matters. We also learned that the ways in which tech managers enforce guidelines can potentially be experienced as paternalistic and disempowering, even as they reduce the cognitive burden of acquiring new literacies. In addition, older adults operate on the threat models of their tech managers, but try to make sense of enforced SP guidelines based on their own pre-established cultural patterns. Finally, we learned that older adults are less inclined to increase their knowledge around SP practices, particular when they are yet to experience harmful consequences of being less informed. In the sections below we elaborate on these takeaways and discuss implications for technology design that can reduce the burden of the above for both the tech managers and the older adults, relating back to our findings as relevant.

5.1 Supporting Tech Managers to Learn, Teach, and Translate

Prior work has extensively studied the different roles played by family members in managing various aspects of digital life within a household [44, 45]. Explaining the existence of roles like *'gurus'* and *'consumers'*, Poole et al.[44] delve into how these roles are assigned to different family members and how the expertise is gained to perform those roles. Along similar lines, our findings revealed that each family had self-appointed 'tech managers' who took responsibility for the SP of the older adults in their household and helped them with technology-related queries. These tech managers were well-versed with using different types of devices and services, but were not necessarily SP experts. Typically, the older adults in these families did not actively engage in SP

conversations in the household. As a result, the SP practices of the entire household were guided by the knowledge of just the non-expert tech managers, who often had significant SP knowledge gaps. The tech managers acknowledged that they found it difficult to understand and explain certain SP concepts, sometimes had to search for solutions on the web when they encountered a SP threat, and their understanding of SP-related concepts often came from news articles and cautionary tales from friends. Some tech managers wished for a safe digital space to learn more about SP, but were unsure where to find such a forum. Others mentioned that they would reach out to members of their extended family or community for help, when needed. Overall, there was acknowledgement that more resources and expertise were needed.

Sometimes the challenge was that the tech managers did not know enough. At other times, the challenge was knowing more than they wished to disclose or discuss with older adults. In such situations, they faced the quandary of not knowing where to draw the line. Prior work has identified similar dynamics of selective guidance of 'helpers' in order to preserve their reputations as experts [45]. In our study, we found that this was not a question of actual tech expertise, but of knowing what the best or most appropriate way of honoring the agency, or recognizing the lack of receptivity or understanding, of the older adults was. The tech managers' motivations to simplify and leave out details that may not seem relevant to older adults were well-placed. However, the decision of what to simplify and leave out is not a straightforward one to make, and the tech managers could be supported in this regard.

We found several participants to serve as tech managers *by proxy*. That is, they expressed a desire to assist older adults from extended families and communities with SP, which was particularly necessary when these older adults' actual tech managers lived far away, sometimes in different countries. Our tech manager participants stepped into that role and acted as community SP stewards by solving these older adults' SP issues. On occasion, they also consulted with the actual tech managers of these older adults in other countries to better understand their SP concerns, reassure them, and act as SP intermediaries when needed.

The scenarios above highlight three opportunities for supporting tech managers in their roles. First, making SP resources accessible and available to them, as *learning* pathways, could reduce their burden and allow them to fulfill their roles with greater ease. Second, providing *teaching* pathways such that they are able to provide assistance in ways that do not infantilize or disempower, and be supported in introducing complex constructs in ways that promote receptivity, could make a difference. Finally, given that many tech managers performed their role as intermediaries or proxies, it is evident that this role could be supported through pathways of *translation* that do not necessarily require all trust to be placed in the intermediary. For each of these cases, research and design might explore the possibilities of creating learning environments for the tech managers, leveraging also the opportunities for exchange with close ties, as we saw in our findings *(4.1.4)*. For example, design could assist tech managers within the community to engage with each other, sharing cautionary tales as well as successful strategies for balancing stringent SP guidelines against respecting older adults' digital agency.

5.2 Engaging Stewardship, Avoiding Paternalism

In generating pathways for learning, teaching, and/or translation, it is necessary to engage and support stewardship, avoiding paternalism. Tech managers established SP guidelines, assisted older adults in their family with SP, and monitored and managed their use of smart devices because they perceived older adults as having limited digital literacies and therefore, high vulnerability to SP threats. These behaviors sometimes manifested as making changes to older adults' SP settings, performing actions on their behalf, and controlling the way they represented themselves on digital platforms. Tech managers controlled older adults' devices and accounts with the intention of

allowing them to explore different types of services while not having to worry about SP. Sometimes, they modified the older adults' SP settings in a manner that made it difficult for the latter to revert those settings without help—these actions were never intentionally malicious, but were often done with the knowledge that they would negatively impact older adults' digital agency. We also found instances where social media settings of older adults were changed so that nobody could see their posts, which were sometimes unintentional or embarrassing—e.g., the name of someone they were intending to search—to increase their freedom to do whatever they want on the platform without social repercussions. They also made the older adults invisible in the process. In such cases, the tech managers unilaterally decided what was best for the older adult without consulting them or explaining their actions. This absolute stewardship borders on paternalism—it reduces older adults' digital agency, and reduces their self efficacy when it comes to technology usage. Prior work studied similar 'paternalism' baked into health technology designed for aging populations and has uncovered the scenarios where privacy from stewards was essential for those populations [36].

5.3 Escaping the Cycle of Low Literacies

Prior work has shown that digital literacies are relatively lower among older adults and that experience with technology can help to augment them [52]. However, the research argues that this augmentation relies on a support infrastructure that includes and extends beyond one's family and friends. We similarly found that our older adult participants had limited digital and SP literacies, but family support offered in the form of paternalistic stewardship did not always help them gain experience or independence. On the contrary, it resulted in fewer opportunities for these adults to gain greater experience and practice their digital skills to their fulfillment.

The older adults we interviewed were evidently less accustomed to managing their own SP by changing their passwords, reverting settings put in place by tech managers, or updating personal information among other things. They also did not voice the need to learn about SP on new apps and services. This is likely because there was always someone else (the tech manager) to take care of the 'boring' or 'difficult' parts associated with SP, such that not only did they not have these skills/practices, they did not experience the need to cultivate them either. In other words, we observed a cycle of low digital and SP literacies that could be challenging to get out of: tech managers of the household attend (perhaps too closely) to the low SP literacies of older adults, leading to reduced incentive for the latter to engage in enhancing their own skills. Researchers have argued that augmenting older adults' digital and SP literacy through different types of educational endeavors can improve their SP behavior [15, 32, 33, 47, 48]. However, in the context of the collaborative SP practices that we studied, it is unclear that such education is even desired.

Tools that are designed to teach older adults in such settings about SP concepts and practices must make the need for SP explicit, clearly illustrating the consequences of not adopting such behaviors. To make such learning attractive, it may be integrated into content, programming, and media that they currently enjoy, rather than developing a separate program, curriculum, or even an advertisement just about SP. One such system might introduce tidbits of SP advice as dialogues between characters in their favorite shows, which would make them learn about SP without explicitly making an effort to do so. Researchers have previously proposed using comics to make privacy notices inviting, engaging, and easy to understand and remember, in an effort to make SP more inclusive and accessible [28]. Interactive tutoring systems that provide just-in-time information about SP as older adults make SP-relevant decisions may also be helpful in improving SP literacy without requiring older adults to change their attitudes towards SP (e.g., a primer about Facebook audience selection controls when they are about to post content on Facebook). These endeavors could help transition older adults' threat models from imposed ones to informed ones. Further, they could provide older adults the structural opportunities needed for informed and long

term adoption of SP guidelines and practices, such that these eventually become an inherent part of older adults' SP practices instead of being unquestioned rules that they follow. This could help gradually dismantle the cycle of low SP literacy and paternalistic stewardship that we observed.

6 CONCLUSION

In this study, we present the first exploration into security and privacy practices of older adults in urban India and unpack the organization of and motivation for collective SP management in this context. We showed how self-appointed family tech managers—many of whom were not SP experts—acted as SP stewards for older adults. In so doing, these non-expert tech managers imposed their threat models onto older adults by creating and enforcing stringent guidelines for how the older adults in their care could use digital technologies, often without consent or explanation. In turn, this paternalistic stewardship reduced older adults' digital agency and self-efficacy. Older adults would sometimes subvert these guidelines, but, for their part, felt no need to improve their own SP literacy because of the SP stewardship of their family tech managers. Based on these findings, we synthesized design implications for technologies that better support SP stewardship, but afford both stewards and those under their care more opportunities to enhance SP literacy and digital agency.

ACKNOWLEDGMENTS

We are thankful to our participants for taking the time to talk to us and for sharing their experiences. We also thank Aprameya Satish, and all our colleagues from the TanDEm Lab at Georgia Tech for their invaluable support and feedback. Finally, we thank our anonymous reviewers for their insightful feedback and encouragement throughout the review process. Some of the work on this paper was generously funded by NSF SaTC Award 1755625.

REFERENCES

[1] Syed Ishtiaque Ahmed, Md Romael Haque, Jay Chen, and Nicola Dell. 2017. Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–20.

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

[3] Irwin Altman. 1977. Privacy regulation: Culturally universal or culturally specific? *Journal of social issues* 33, 3 (1977), 66–84.

[4] Yahel Ben-David, Shaddi Hasan, Joyojeet Pal, Matthias Vallentin, Saurabh Panjwani, Philipp Gutheim, Jay Chen, and Eric A Brewer. 2011. Computing security in the developing world: A case for multidisciplinary research. In *Proceedings of the 5th ACM workshop on Networked systems for developing regions*. 39–44.

[5] Hichang Cho, Bart Knijnenburg, Alfred Kobsa, and Yao Li. 2018. Collective privacy management in social media: A cross-cultural validation. *ACM Transactions on Computer-Human Interaction (TOCHI)* 25, 3 (2018), 1–33.

[6] Hichang Cho, Milagros Rivera-Sánchez, and Sun Sun Lim. 2009. A multinational study on online privacy: global concerns and local responses. *New media & society* 11, 3 (2009), 395–416.

[7] Chhaya Chouhan, Christy M LaPerriere, Zaina Aljallad, Jess Kropczynski, Heather Lipford, and Pamela J Wisniewski. 2019. Co-designing for Community Oversight: Helping People Make Privacy and Security Decisions Together. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–31.

[8] Cassandra Cross. 2017. 'But I've never sent them any personal details apart from my driver's licence number…': Exploring seniors' attitudes towards identity crime. *Security Journal* 30, 1 (2017), 74–88.

[9] Sauvik Das. 2016. Social cybersecurity: Understanding and leveraging social influence to increase security sensitivity. *it-Information Technology* 58, 5 (2016), 237–245.

[10] Sauvik Das, Laura A Dabbish, and Jason I Hong. 2019. A typology of perceived triggers for end-user security and privacy behaviors. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*.

[11] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. 2014. The effect of social influence on security sensitivity. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*. 143–157.

[12] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I Hong. 2018. Breaking! A Typology of Security and Privacy News and How It's Shared. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–12.

[13] Paul Dourish, Rebecca E Grinter, Jessica Delgado De La Flor, and Melissa Joseph. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing* 8, 6 (2004), 391–401.

[14] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. 2016. Do or do not, there is no try: user engagement may not improve security outcomes. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*. 97–111.

[15] 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)*.

[16] Shirley Gaw, Edward W Felten, and Patricia Fernandez-Kelly. 2006. Secrecy, flagging, and paranoia: adoption criteria in encrypted email. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 591–600.

[17] Galen A. Grimes, Michelle G. Hough, Elizabeth Mazur, and Margaret L. Signorella. 2010. Older Adults' Knowledge of Internet Hazards. *Educational Gerontology* 36, 3 (2010), 173–192. https://doi.org/10.1080/03601270903183065 arXiv:https://doi.org/10.1080/03601270903183065

[18] Rebecca E Grinter, W Keith Edwards, Marshini Chetty, Erika S Poole, Ja-Young Sung, Jeonghwa Yang, Andy Crabtree, Peter Tolmie, Tom Rodden, Chris Greenhalgh, et al. 2009. The ins and outs of home networking: The case for useful and usable domestic networking. *ACM Transactions on Computer-Human Interaction (TOCHI)* 16, 2 (2009), 1–28.

[19] Rebecca E Grinter, W Keith Edwards, Mark W Newman, and Nicolas Ducheneaut. 2005. The work to make a home network work. In *ECSCW 2005*. Springer, 469–488.

[20] Francisco J Gutierrez and Sergio F Ochoa. 2017. It takes at least two to tango: understanding the cooperative nature of elderly caregiving in Latin America. In *Proceedings of the 2017 ACM Conference on computer supported cooperative work and social computing*. 1618–1630.

[21] Rayna Hollander. 2017. There's a data explosion happening in India — and Jio is at the center of it. https://www.businessinsider.com/jio-india-data-explosion-2017-7

[22] Adele E Howe, Indrajit Ray, Mark Roberts, Malgorzata Urbanska, and Zinta Byrne. 2012. The psychology of security for the home computer user. In *2012 IEEE Symposium on Security and Privacy*. IEEE, 209–223.

[23] Margaret C Jack, Pang Sovannaroth, and Nicola Dell. 2019. " Privacy is not a concept, but a way of dealing with life" Localization of Transnational Technology Platforms and Liminal Privacy Practices in Cambodia. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–19.

[24] Nimisha Jain, Kanika Sanghi, and Ankur Jain. 2019. Ten Trends That Are Altering Consumer Behavior in India. https://www.bcg.com/en-us/publications/2019/ten-trends-altering-consumer-behavior-india

[25] Haiyan Jia and Heng Xu. 2016. Autonomous and interdependent: Collaborative privacy management on social networking sites. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 4286–4297.

[26] Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. 2014. Privacy attitudes of mechanical turk workers and the us public. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*. 37–49.

[27] Naveena Karusala, Apoorva Bhalla, and Neha Kumar. 2019. Privacy, Patriarchy, and Participation on Social Media. In *Proceedings of the 2019 on Designing Interactive Systems Conference*. 511–526.

[28] Bart Knijnenburg and David Cherry. 2016. Comics as a medium for privacy notices. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*.

[29] Sandhya Krishnan and Neeraj Hatekar. [n.d.]. *Rise of the New Middle Class in India and Its Changing Structure*. https://www.epw.in/journal/2017/22/special-articles/rise-new-middle-class-india-and-its-changing-structure.html

[30] Ponnurangam Kumaraguru and Lorrie Cranor. 2005. Privacy in India: Attitudes and awareness. In *International workshop on privacy enhancing technologies*. Springer, 243–258.

[31] Rohit KVN. 2020. Apple records stellar growth in iPhone, iPad sales in India. https://www.deccanherald.com/business/technology/apple-records-stellar-growth-in-iphone-ipad-sales-in-india-799225.html

[32] Nicole M Lee. 2018. Fake news, phishing, and fraud: a call for research on digital media literacy education beyond the classroom. *Communication Education* 67, 4 (2018), 460–466.

[33] Nigel Martin and John Rice. 2013. Spearing high net wealth individuals: the case of online fraud and mature age internet users. *International Journal of Information Security and Privacy (IJISP)* 7, 1 (2013), 1–15.

[34] 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.

[35] Nora McDonald, Alison Larsen, Allison Battisti, Galina Madjaroff, Aaron Massey, and Helena Mentis. 2020. Realizing Choice: Online Safeguards for Couples Adapting to Cognitive Challenges. In *Sixteenth Symposium on Usable Privacy and Security ({SOUPS} 2020)*. 99–110.

[36] Andrew McNeill, Pam Briggs, Jake Pywell, and Lynne Coventry. 2017. Functional privacy concerns of older adults about pervasive health-monitoring systems. In *Proceedings of the 10th International Conference on PErvasive Technologies Related to Assistive Environments*. 96–102.

[37] 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.

[38] Helena M Mentis, Galina Madjaroff, and Aaron K Massey. 2019. Upside and downside risk in online security for older adults with mild cognitive impairment. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[39] Sharan B Merriam. 2002. Merriam, Sharan B., ed., Qualitative Research in Practice: Examples for Discussion and Analysis. San Francisco: Jossey-Bass, 2002. (2002).

[40] James Nicholson, Lynne Coventry, and Pamela Briggs. 2019. " If It's Important It Will Be A Headline" Cybersecurity Information Seeking in Older Adults. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–11.

[41] Daniela Oliveira, Harold Rocha, Huizi Yang, Donovan Ellis, Sandeep Dommaraju, Melis Muradoglu, Devon Weir, Adam Soliman, Tian Lin, and Natalie Ebner. 2017. Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 6412–6424.

[42] Sameer Patil, Alfred Kobsa, Ajita John, and Doree Seligmann. 2010. Comparing privacy attitudes of knowledge workers in the US and India. In *Proceedings of the 3rd international conference on Intercultural collaboration*. 141–150.

[43] Anne Marie Piper, Raymundo Cornejo, Lisa Hurwitz, and Caitlin Unumb. 2016. Technological caregiving: Supporting online activity for adults with cognitive impairments. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 5311–5323.

[44] Erika Shehan Poole, Marshini Chetty, Rebecca E Grinter, and W Keith Edwards. 2008. More than meets the eye: transforming the user experience of home network management. In *Proceedings of the 7th ACM conference on Designing interactive systems*. 455–464.

[45] Erika Shehan Poole, Marshini Chetty, Tom Morgan, Rebecca E Grinter, and W Keith Edwards. 2009. Computer help at home: methods and motivations for informal technical support. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 739–748.

[46] Indira Jai Prakash. 1999. *Ageing in India*. Technical Report. World Health Organization Geneva.

[47] Anabel Quan-Haase and Isioma Elueze. 2018. Revisiting the privacy paradox: Concerns and protection strategies in the social media experiences of older adults. In *Proceedings of the 9th International Conference on Social Media and Society*. 150–159.

[48] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J Aviv. 2019. " Woe is me" Examining Older Adults' Perceptions of Privacy. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–6.

[49] Jennifer A Rode and Erika Shehan Poole. 2018. Putting the gender back in digital housekeeping. In *Proceedings of the 4th Conference on Gender & IT*. 79–90.

[50] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. 2018. " Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*. 127–142.

[51] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. 2017. Self-confidence trumps knowledge: A cross-cultural study of security behavior. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 2202–2214.

[52] Kathleen Schreurs, Anabel Quan-Haase, and Kim Martin. 2017. Problematizing the digital literacy paradox in the context of older adults' ICT use: Aging, media discourse, and self-determination. *Canadian Journal of Communication* 42, 2 (2017).

[53] Irving Seidman. 2006. *Interviewing as qualitative research: A guide for researchers in education and the social sciences*. Teachers college press.

[54] Anna Cinzia Squicciarini, Mohamed Shehab, and Federica Paci. 2009. Collective privacy management in social networks. In *Proceedings of the 18th international conference on World wide web*. 521–530.

[55] Anna C Squicciarini, Heng Xu, and Xiaolong Zhang. 2011. CoPE: Enabling collaborative privacy management in online social networks. *Journal of the American Society for Information Science and Technology* 62, 3 (2011), 521–534.

[56] Sakari Taipale. 2019. *Intergenerational connections in digital families*. Springer.

[57] Economic Times. 2018. India smartphone growth likely in double digits in 2018: IDC. https://economictimes.indiatimes.com/tech/hardware/india-smartphone-growth-likely-in-double-digits-in-2018-idc/articleshow/64157987.cms

[58] Peter Tolmie, Andy Crabtree, Tom Rodden, Chris Greenhalgh, and Steve Benford. 2007. Making the home network at home: Digital housekeeping. In *ECSCW 2007*. Springer, 331–350.

[59] Aditya Vashistha, Richard Anderson, and Shrirang Mare. 2018. Examining security and privacy research in developing regions. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*. 1–14.

[60] John Vines, Gary Pritchard, Peter Wright, Patrick Olivier, and Katie Brittain. 2015. An age-old problem: Examining the discourses of ageing in HCI and strategies for future research. *ACM Transactions on Computer-Human Interaction (TOCHI)* 22, 1 (2015), 1–27.

[61] Hue Watson, Eyitemi Moju-Igbene, Akanksha Kumari, and Sauvik Das. 2020. " We Hold Each Other Accountable": Unpacking How Social Groups Approach Cybersecurity and Privacy Together. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–12.

[62] Stephen D Weaver and Mark Gahegan. 2007. Constructing, visualizing, and analyzing a digital footprint. *Geographical Review* 97, 3 (2007), 324–350.

[63] Daricia Wilkinson, Moses Namara, Karla Badillo-Urquiola, Pamela J Wisniewski, Bart P Knijnenburg, Xinru Page, Eran Toch, and Jen Romano-Bergstrom. 2018. Moving Beyond a" one-size fits all" Exploring Individual Differences in Privacy. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–8.

[64] Lei Xu, Chunxiao Jiang, Nengqiang He, Zhu Han, and Abderrahim Benslimane. 2018. Trust-based collaborative privacy management in online social networks. *IEEE Transactions on Information Forensics and Security* 14, 1 (2018), 48–60.