Towards Building Community Collective Efficacy for Managing Digital Privacy and Security within Older Adult Communities

JESS KROPCZYNSKI, University of Cincinnati
ZAINA ALJALLAD, University of Central Florida
NATHAN JEFFREY ELROD, University of Cincinnati
HEATHER LIPFORD, University of North Caroline Charlotte
PAMELA J. WISNIEWSKI, University of Central Florida

Older adults are increasingly becoming adopters of digital technologies, such as smartphones; however, this population remains particularly vulnerable to digital privacy and security threats. To date, most research on technology used among older adults focuses on helping individuals overcome their discomfort or lack of expertise with technology to protect them from such threats. Instead, we are interested in how communities of older adults work together to collectively manage their digital privacy and security. To do this, we surveyed 67 individuals across two older adult communities (59 older adults and eight employees or volunteers) and found that the community's collective efficacy for privacy and security was significantly correlated with the individuals' self-efficacy, power usage of technology, and their sense of community belonging. Community collective efficacy is a group's mutual belief in its ability to achieve a shared goal. Using social network analysis, we further unpacked these relationships to show that many older adults interact with others who have similar technological expertise, and closer-knit older adult communities that have low technology expertise (i.e., low power usage and self-efficacy) may increase their community collective efficacy for privacy and security by embedding facilitators (e.g., employees or volunteers) who have more technical expertise within their communities. Our work demonstrates how both peer influence and outside expertise can be leveraged to support older adults in managing their digital privacy and security.

CCS Concepts: • **Human-centered computing → Social network analysis**.

Additional Key Words and Phrases: Community Collective Efficacy; Self-Efficacy; Power Users; Privacy and Security; Older Adults

ACM Reference Format:
Jess Kropczynski, Zaina Aljallad, Nathan Jeffrey Elrod, Heather Lipford, and Pamela J. Wisniewski. 2020. Towards Building Community Collective Efficacy for Managing Digital Privacy and Security within Older Adult Communities. In *CSCW '20: ACM Conference on Computer Supported Cooperative Work and Social Computing, October 17–21, 2020, Minneapolis, MN*. ACM, New York, NY, USA, 27 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Older adults (ages 65 plus) make up 7% of the world's population, a number that is expected to increase more than 60 percent by 2030 [49]. While we often think of older adults as late adopters of technology, nearly two-thirds of older adults in the U.S. go online and 42% own a smartphone.

CSCW '20, October 17–21, 2020, Minneapolis, MN

ACM ISBN 978-1-4503-9999-9/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

Yet, despite the wide adoption of smartphones, Pew Research reveals that most older adults report needing help setting up these devices, and 34% say they have little or no confidence in their ability to use them [1]. Older adults are often considered the least adaptable to novel technologies [49], and thus, are regularly the targets of cybercrimes, such as identity theft and fraud [51]. As such, Huang and Bashir [30] identified a "privacy divide" among older adults, finding that they take fewer privacy protective actions than younger adults, and conclude that researchers and designers should work to build privacy-friendly systems that are easy-to-use in order to accommodate for the lack of technology expertise of older adults. This narrative, which is fairly prevalent in existing literature (e.g., [6, 23, 37]), suggests that older adults are at-risk for digital privacy and security threats due to their lack of technology expertise, necessitating the development of easier-to-use and better designed technologies. In contrast, we are interested in understanding how we might increase older adults' perceived personal capacity, or self-efficacy [2], in managing their digital privacy and security when using novel technologies. As opposed to making simplified technologies for older adult communities, we seek to explore how technological literacy can be embedded and distributed in a way that empowers them.

This study leverages the concept of *community oversight* [15] as a mechanism for helping older adults collectively manage their digital privacy and security. In our prior work [15], we developed this framework of community oversight as a means to help individuals increase their capacity for making digital privacy and security decisions together by drawing on the expertise and bidirectional feedback garnered within one's social network. In this paper, we build upon the framework by examining and operationalizing this capacity for digital privacy and security as Carroll's [12, 13] construct of *community collective efficacy*, which is an extension of an individual's self-efficacy [2] and refers to the capacity or ability of a group towards accomplishing a shared goal. We study community collective efficacy in the novel context of digital privacy and security. Building upon these foundational concepts, we pose the following research questions:

RQ1: *What individual (i.e., self-efficacy, power usage), community (i.e., sense of community belonging), and network-level factors (i.e., homophily) influence the formation of community collective efficacy for digital privacy and security?*

RQ2: *When community collective efficacy is low among members of a community, how might technology expertise be introduced in order to increase collective capacity to co-manage privacy and security?*

To answer these research questions, we conducted a web-based survey of 67 individuals embedded within two older adult communities. One community was a residential community (N = 37 older adults; N = 5 employees), while the other was a socially constructed community of individuals participating in social and educational programming at a senior center (N = 22 older adults; N = 3 volunteers). We leveraged social network analysis techniques to study and report on the structure of these communities. Specifically, we modeled network connections and measured individual-level (i.e., self-efficacy and power usage) and community-level (i.e., sense of community belonging) factors that contributed to the communities' collective efficacy for digital privacy and security. We found that the individual and community-level factors were all significantly correlated with community collective efficacy to the extent that an individual having low scores on one of these scales was correlated with low scores on all scales. Further, we found that the residential community, which had high community collective efficacy for privacy and security, were supported by group facilitators who characterized themselves as having high digital literacy (i.e., high scores for power usage and self-efficacy for privacy and security). This suggest potential for being able to interject technology expertise into older adult communities in a way that can increase the collective efficacy for the entire community.

This study makes a unique contribution to the CSCW research community by studying digital privacy and security in the context of older adult communities and their collective capacity to support one another in managing their digital privacy and security together. It provides a better understanding of collective sense making and social support for digital privacy and security among older adults within two communities. We develop a framework to better understand how older adults collaborate and provide digital privacy and security oversight to one another. We apply social network analysis as a novel way to study communities of users and their individual and collective capacity for managing their digital privacy and security. We inform future interventions that could positively impact society by protecting older adults from vulnerabilities that stem from making decisions about privacy and security settings in isolation and possibly reduce their susceptibility to online threats.

2 BACKGROUND

In this section, we first synthesize the literature related to older adults and their digital privacy and security. Then, we connect this research to community-based privacy research that goes beyond the individual to studying groups.

2.1 Older Adults and their Digital Privacy and Security

Adults aged 55 and older are currently one of the fastest-growing demographics to utilize the web as part of their everyday lives [14]. Smartphone usage, in particular, has been a useful tool in closing the digital divide that has long existed for older adults by making technology more accessible and increasing the digital literacy among older generations [28]. Researchers such as Shuijing and Tao [56] have found that privacy awareness and technological expertise of older adults is low compared to other demographics, making them (for example) prone to over-disclose online and placing them at greater risk of privacy and security violations. Others have also found deficits related to older adults and their technology use. In examining common privacy and security threat models, misconceptions, and strategies used by older adults, Frik et al. [26] found that managing concerns frequently consists of limiting or avoiding technology use. In another study, Kurniawan [39] found that older adults are often passive users of mobile phones and preferred features that reduce, rather than increase, the phones' functional capabilities. Similarly, Czaja et al. [18] found that those 65 years and older were less likely to learn new technologies than the younger generations. A study by Knowles and Hanson [36] found that older adults' trust and use of technologies do not go hand-in-hand and their observations of "using-while-distrusting" highlight design opportunities. As a result, studies often emphasize designing systems that are simple and easy-to-use for older adults; such as ones that give real-time and understandable feedback [41].

However, other researchers have begun to move away from these primarily deficit- and fear-based narratives of older adults' technology use and privacy to uncover more nuance. For instance, some research suggests that there is a general tendency for older adults to be more cautious of their digital privacy than younger audiences [31, 48]. Mitzner et al. found that while older adults had negative connotations towards technology, their positive outlook outweighed the negative; older adults enjoyed the convenience and helpful features that come with technology but were concerned about the security and reliability of these devices. Therefore, by addressing the privacy and security concerns of older adults, we may be able to enhance their comfort-level, and subsequently, their adoption and use of technology.

Meanwhile, innovations in the home care and assistive technology domains have sparked interest in older adult populations who are looking for new resources to promote independence with aging [44], showing that some older adults are willing to make privacy trade-offs for maintaining their autonomy [58]. One such study examined the use of a smart device to assist older adults in their

daily lives and found that participants who were regular technology users had fewer concerns about privacy violations [35]. As we look to the future, many see promise for the use of smart home technologies to help a growing population of older adults age-in-place, however, Chung et al. [16] reports that privacy is one of the most important factors that can affect its adoption. McNeill et al. [45] examined health monitoring systems for older adults and find that it appears to be an implicit assumption in the design of these systems that older adults may not need privacy, but interviewing older adults find that is certainly not the case. Caine et al. [10] implemented a medical monitoring system for older adults, which gave them control over how their data was shared. The researchers found that the system provided older adults an effective way to simultaneously maintain their privacy and benefit from in-home monitoring. These studies highlight the complex trade-offs older adults make between autonomy and privacy when adopting and using technology.

While research has emphasized risks and enhancements to technology that can support older adults' daily lives, this research brings attention to the larger socio-technical environment that helps to fill knowledge gaps when using technologies, and its ability to support the digital privacy and security concerns of older adults. In this study, we extend the investigation of technology use to individual and community capacity to manage privacy and security to develop a better understanding of how communities of older adults can work together to address these concerns.

2.2 A Case for Community-Based Privacy Management for Older Adult Communities

As previously mentioned, much of the existing work regarding older adults and their digital privacy and security tends to focus on individual deficits that need to be accommodated through design [39]. In contrast, Yuan et al. [60] explored external factors that impact older adults' personal health and well-being. By studying how social factors impacted their personal well-being, Yuan suggests designing more technologies for communities of older adults through which to interact and connect. Hornung et al. [29] examined older adults' use of an online neighborhood portal and take the position that privacy-related practices are inherently part of socially negotiated boundary management. Their work contributes to the scant empirically grounded research that observes privacy and security issues in elderly people's everyday lives in relation to their social networks and socio-cultural living environments. But it was Mendel [47] who was among the first to suggest leveraging the support of an older adults' social network, especially close-ties such as family and friends, to help them manage the privacy and security of their mobile devices. Mendel's initial dissertation results found that adult children are more than willing to assist older relatives with their technology needs, but the frequency in which this occurs is rare. Similarly, Chakraborty et al. [14] found that social influence can play a key role in older adults' privacy and security decisions. They studied older adult social media users and found that they tend to opt out of sharing personal information on Facebook and that the sharing habits of their friends influenced this behavior. In a field trial of older adults use with mobile technology, Coventry and Briggs [17] found that some respondents found location awareness features to be a potential protective feature while others found it a threat. When convening participants in a focus group, they found evidence of a change of attitude towards the threat of location awareness when participants had the opportunity to discuss the feature together.

More generally, researchers have found promise in leveraging social and community-based influence to help individuals with digital privacy and security decisions. For instance, Das et al. [22] explored how security-feature adoption diffused through social networks. They found that users were more likely to make privacy and security decisions, such as deleting an app or changing a password, if others in their network also did so, but the likelihood of security-feature adoption was much higher when these behaviors were physically observable. As a result, Das [20] later laid the foundations of *social cybersecurity* as a theoretical framework for leveraging peer influence

to raise the awareness of privacy and security tools, as well as the motivation to use them. Social cybersecurity extends beyond transparency in personal security-feature adoption to advice-giving and receiving. Dourish et al. [24] found that when technology users need advice, they turn to trusted family and friends who they believe have the necessary expertise. These findings are consistent with other studies that observed that individuals rely on their family and peer groups when in need of digital privacy and security advice [21, 53].

We have previously proposed a model of Community Oversight for helping people manage their digital privacy and security together [15]. Using participatory design methods, they asked small groups of people who knew one another to design a mobile app to instantiate their model. Key components of this model included two levels of participation: 1) Individuals: the willingness to share one's personal experiences with others, and 2) Community: The interconnectedness of individuals to form a group that provides oversight of one another. These two levels of community oversight were facilitated through transparency, trust, and awareness between the individuals within the community. In their study, they found that older adults were more reluctant to give oversight to others but were receptive to receiving it. We build upon and extend this work by studying individual-level and community-level factors that contribute to the formation of community collective efficacy for older adults when making privacy and security decisions related to smartphone use. We believe that tools to support social privacy and security in older adult communities require an understanding of the community dynamics within these groups and distribution of technological expertise within social networks of older adults. The following section describes our framework to investigate such dynamics.

3 A FRAMEWORK FOR BUILDING COMMUNITY COLLECTIVE EFFICACY FOR PRIVACY AND SECURITY

In Figure 1, we propose a theoretical framework for building community collective efficacy for privacy and security. In the sections below, we define each of the constructs in our model.

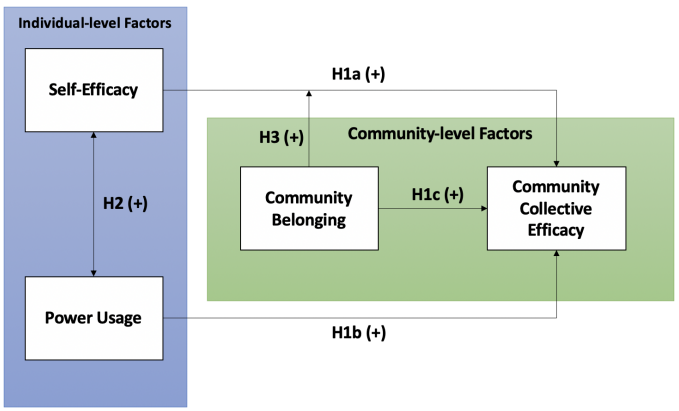

Fig. 1. Research Framework of Building Community Collective Efficacy for Digital Privacy and Security

3.1 Community Collective Efficacy for Privacy and Security

Community collective efficacy was first introduced to the Human-Computer Interaction (HCI) research community by Carroll et al. [12, 13], after identifying the need to robustly measure the collective beliefs of collaborative groups when assessing their capacity to carry out shared

computing related tasks. The researchers modeled this construct as an extension of Bandura's construct of self-efficacy [2], which is described in more detail in the sections below. Collective efficacy refers to beliefs about collective capacities in specific domains. For instance, HCI researchers have utilized Carroll et al.'s conceptualization of community collective efficacy predominantly in the HCI subdomain of community informatics [32–34], finding that collective efficacy is positively related with both offline and online community activities.

Another domain where collective efficacy is often evoked is in the neighborhood watch [5], which can demonstrate a community's capacity to work together to achieve public safety. Carbone et. al found individuals who perceived neighborhoods more positively and had strong social ties played an important role in collective efficacy [11]. Beck et al. argued that if strategies were implemented for communities to focus on building a greater collective efficacy, neighborhood violence and the crime rate would decrease [4]. These studies have agreed that collective efficacy can result in safer spaces and better relationships between community members. Yet, ours is the first study in HCI to apply the concept of community collective efficacy to the specific domain of digital privacy and security. We measure collective efficacy as our dependent variable to understand how older adults perceive their community's capacity to work together to make digital privacy and security decisions related to smartphones. Comparing community collective efficacy for privacy and security to those of an individual's self-efficacy for privacy and security, their power usage, and sense of community belonging will help us understand how these communities operate. Next, we unpack the individual and community-level constructs that we believe influence the collective efficacy for privacy and security within older adult communities.

3.2 Self-Efficacy for Privacy and Security

According to Bandura [2], self-efficacy is defined by how well one perceives their own personal ability to execute courses of action required to deal with prospective situations. In his guide to creating adaptable self-efficacy scales for specific domains [2], Bandura explained that this can simply be done by defining the domain in which to measure one's perceived capabilities (e.g., making decisions about one's digital privacy and security). Previous research has found self-efficacy to be a factor in healthy aging practices among older adults [55] and a factor in participation in physical and social activities [52]. Self-efficacy has been found to be positively correlated with community collective efficacy when it comes to addressing civic matters [12, 13]. Franz et al.[25] found that age, rather than gender, was a significant factor in the comfort level of learning a new technology; they found that older adults had significantly lower levels of self-efficacy and tended to ask more questions than younger adults in this context. Czaja et al. [19] studied technology use over time and found that while the self-efficacy of older adults did not seem to change, their use and adoption of technology has. Thus, they conclude more research should examine such factors when studying the adoption and use of technology by older adults. Based on this past literature, it follows that an older adult with high levels of self-efficacy for privacy and security will contribute to the community's collective efficacy for privacy and security. Therefore, we hypothesize:

H1a: *Self-efficacy for privacy and security will be positively associated with community collective efficacy for privacy and security.*

Next, we explain the importance of one's perception of their own technology expertise in relation to self-efficacy and collective efficacy for privacy and security.

3.3 Technology Expertise and Power Usage

As shown in our related work, one's level of technological expertise and comfort-level using technology play a key role in privacy management, especially for older adults. As such, we incorporated Power Usage as a construct in our model. Sundar et. al [57] describes power users as proactive

technology users who are more likely to explore all possible customizations with their technology. Marathe et al. [43] drew from five disciplines (psychology, information sciences, media effects, marketing, and consumer research) to define the concept of technology power users based on their high usage in motivation, expertise, efficacy, and behavior with their technology. In follow up studies by Sundar and Maranthe [57], they found interesting relationships between power usage and privacy; privacy was a key factor in users' attitudes towards personalization and customization, and power users consistently rated systems higher when they had a customizable interface. We draw this prior research on power users to understand how the presence of people with high knowledge and comfort using technology within a self-selected social network will affect connected others' overall community collective efficacy scores. Specifically, we hypothesize:

H1b: *Power usage will be positively associated with community collective efficacy for privacy and security.*

H2: *Power usage will be positively associated with one's self-efficacy for privacy and security.*

In summary, we believe that self-efficacy and power usage are two individual-level factors that will influence one another and the overall community's level of collective efficacy for privacy and security. Next, we introduce the concept of sense of belonging within one's community and how it may influence these relationships.

3.4 Community Belonging

Community capacity to take action together on issues that impact the lives on members of the community begins with individuals that feel a sense of belonging to a community. Carroll's [13] research found sense of community belonging and community activism to be highly correlated with community collective efficacy. A given individual may perceive him- or herself to have capacity to manage their own privacy and security (i.e. high self efficacy for privacy and security), but a lack of community belonging may impact their perception that their community has the capacity to manage such tasks together. Sense of community belonging is used in our framework to measure participants' perceived connection to their community, independent of individual capacity to manage privacy and security. It stands to reason that if a participant does not have a strong sense of belonging to the self-selected group in their social network, he or she would not feel strongly about the communities' collective capacity to address privacy and security together.

Thus, we posit:

H1c: *Sense of community belonging will be positively associated with community collective efficacy for privacy and security.*

H3: *Sense of community belonging moderates the relationship between self-efficacy and community collective efficacy, such that high levels of community belonging will strengthen the positive relationship between the two.*

3.5 Community Level Network Effects

Further, social networks have a tendency towards similarity among individuals that associate with one another, called homophily [46]. For example, group members may be similar in age, personal interests, or other characteristics. It stands to reason that members of older adult communities will share similarities based on demographic questions and will also share similarities in perceived community collective efficacy or other constructs. Therefore, also we hypothesize that homophily may be present within older adult communities:

H4: *Homophily will be present within communities based on demographic or construct similarity.*

In our methods, we describe the design of a web-based survey study of older adults to validate our theoretical model of community collective efficacy for privacy and security and test our hypotheses.

4 METHODS

In this section, we provide an overview of our study, followed by an explanation of how we operationalized each of the constructs presented in our research model. We conclude by describing the data analysis approach we used to answer each of our research questions and hypotheses.

4.1 Study Overview and Participant Recruitment

Our research aims to understand older adults' perceptions of their individual and community-level capacity for making digital privacy and security decisions and how these perceptions are distributed within their communities. Therefore, we conducted a web-based social network analysis survey study of two older adult communities. Participants were recruited from two different communities located in two different states in the Midwest and Southeastern parts of the United States. Members of the research team also participated in a typical in-person meeting or gathering where the majority of members would be present to explain the nature of the research in-person and describe the importance of listing others names clearly on the social network portion of the survey. At that time, participants were given the option to complete a paper-based survey if they were uncomfortable with the online survey method; however, no participants elected for this option. The overlapping clusters of self-selected groups make up the whole of the two networks. Data were collected from these communities between February 2019 and August 2019.

An important first step to social network analysis is to identify a logical community boundary that exists based on self-organized groups in order to map social connections among all members of the network [40]. Therefore, we designed our study to enroll complete clusters that form a networked community. Participants were recruited by contacting local older adult communities near our respective universities. We explained to organizers that we were seeking small clusters of at least 5-10 people in communities such as friend groups, clubs, or other groups that meet regularly and would be willing to participate in the survey together. We received Institutional Review Board (IRB) approval from both universities involved in this research to conduct this study. Prior to participating in our study, participants were asked to agree to participate as part of a community after being presented with an explanation of the research in person, and individually consented to participation within the survey itself. We describe the design of the survey and the operationalization of our model constructs in the next section.

4.2 Survey Design and Operationalization of Constructs

We used Qualtrics as the web-based platform for the survey. In the preamble to the survey, we described the study as an investigation into the ways that communities work together to manage digital privacy and security. Within the survey, privacy was defined to participants as "activities to keep yourself and loved ones safe from uninvited attention and scrutiny online." Security was defined as "activities to protect online data such as financial data (credit cards, accounts), healthcare data, and personally identifiable information." After participants were oriented to the purpose of the survey, they were presented with the survey questions divided into four parts. In the first part, participants completed an open response format social network questionnaire [9], which asked them to list the names of the members of their community who they interacted with on a daily basis (first name and last initial for matching purposes among community members). Second, we asked them to complete the community-level scales for collective efficacy for privacy and security and sense of community belonging. Third, they responded to the individual-level scales related to self-efficacy for privacy and security and power usage. Finally, participants provided basic demographic information to contextualize their responses.

These activities altogether took approximately 15-30 minutes. A code for an $10 Amazon gift card was emailed to each participant as they completed the survey using the same email address they provided to receive the survey link. In the subsections below, we describe how we measured each of the constructs presented in our model, and we also included all scale items in Appendix A. For all measures, participants were presented statements and were asked to rate each on a 5-point Likert scale from 1 (strongly disagree) to 5 (strongly agree), consistent with the way these questions have been presented in previous work.

4.2.1 Community Collective Efficacy for Privacy and Security. Carroll et al.[13] describe this scale as a "capacity analysis" of the community to succeed in joint ventures. Our work adapts this construct to measure older adult communities perceived collective capacity to manage privacy and security together. To accomplish this, each item was phrased as a challenge or achievement in privacy and security management, as a collective capacity (e.g. "Despite other obligations, we can find time to discuss our decisions about digital privacy and security management"). Participants were asked here to draw from the definitions of privacy and security management described earlier in the survey. The composite score of this scale was used to examine an individuals' perception of community capacity to manage privacy and security together. RQ1 relates to the formation of community collective efficacy; therefore, we investigated the associated factors below that may support higher levels of community-collective efficacy as our dependent variable.

4.2.2 Self Efficacy for Privacy and Security. An abbreviated version of Bandura's [2] self-efficacy scale was employed, with each item adapted to engage users in the domain of digital privacy and security (e.g. "Online privacy and security decision-making is not too complicated for me to understand").

4.2.3 Power Usage. We utilized Sundar's pre-validated scale of Power Usage [57] (e.g. "Using any technological devices comes easy to me") as a proxy measure for one's level of technology expertise. Some questions in this scale referenced types of technology that were outdated such as a PDA; therefore, we modernized these references by replacing this with a references such as this one with an equivalent such as a smartphone. This scale also served as an individual-level factor in our model that may be associated with community collective efficacy.

4.2.4 Community Belonging. Carroll's initial work on community collective efficacy [12] investigated external construct validity by understanding the collective capacity's relationship to variables derived from community involvement. Therefore, the community belonging variables were adapted from Carroll et al. [12] (e.g. "I belong in this community"). These items were used to understand an individuals' sense of community belonging, prior to engaging with questions about community capacity to address privacy and security challenges.

4.3 A Social Network Analysis Approach

The previous section describes measured concepts at the individual (i.e., self-efficacy and power usage), community (sense of community belonging) and network levels (homophily) to understand their relationships with community collective efficacy for privacy and security. In the following section the social network analysis techniques used to examine the social network data are briefly expanded upon.

Social network analysis (SNA) creates opportunities to quantify and visualize social characteristics of communities and the individuals within them [9]. SNA graphing techniques visualize nodes (representing individuals) connected by links (indicating social relationships) to analyze the presence, direction, and types of ties in a community [54]. Each individual (or node) in a network may contain attribute information, such as gender, age, or other characteristics of an individual.

In our current context, the nodes in the networks represent the individual community members with the links representing people in their community that they interact with on a daily basis. We utilize both demographic information as well as the constructs from our framework to model attributes of the individuals within each community. The total number of community members across communities was 88 older adults, we adopted the list-wise deletion method and only accepted complete and valid responses to surveys from complete self-selected groups yielding a total of 67 total participants.

To prepare the survey data for analysis, we first created a composite score for each scale by averaging across all survey items for each construct. Given that questions were asked on a 5-point scale and our interest is in similarity in responses among community members to examine network effects, further reduction was applied to convert continuous scores to categorical variables based on high, medium (or average), and low composite scores. To create these categorical variables, we used tertiary mean split based on one standard deviation from the mean. Connections among participants reporting daily interactions on our survey were converted into a one-mode directed sociomatrix of who interacts with whom. This was matched with demographic and construct responses from other survey responses in UCINET for Windows [8], the social network analysis software where all analyses were performed.

Node level network measures also helped us understand simple descriptive statistics of the network such as the average number of connections that individuals had, specifically, degree of centrality is used to count the number of links incident upon a node. An additional whole network measure that was examined is overall centralization of each of the two networks. This suite of network measures was used to help us understand the impact that individuals with technical expertise have on a network from the individual level.

Next, we investigated the individual- and community-level factors that influence the formation of community collective efficacy for privacy and security (RQ1). To answer RQ1 and test the research hypotheses in our research framework (H1-H3), we conducted a correlation analysis using a quadratic assignment procedure (QAP) [9]. QAP is an adaptation of traditional correlation tests that meets the special conditions of network data (i.e. does not contain a normal distribution or independent observations). QAP correlation was used to calculate measures of association between the relations in attribute matrices. The test compares observed associations to random permutations of comparable matrices to develop standard errors to test for the significance of association.

To test H4, we assessed homophilous tendencies within the two groups. Homophily is the tendency for individuals to be linked to others with similar attributes to their own (i.e. women interacting with other women), while heterophily is a tendency for individuals to be linked to others with different attributes to their own (i.e. women interacting with men) [46]. A measure of homophily is the E-I (external - internal) Index. In this index E represents external ties to a group, based on a categorical attribute of a node (e.g., those of a different gender); I represents internal ties (e.g., those of the same gender). The index is the number of ties external to the groups minus the number of ties that are internal to the group divided by the total number of ties [38]. The resulting number provides an indication of a tendency toward homophily (i.e. network's preference for internal ties) or a tendency towards heterophily (i.e. network's preference for external ties). The resulting index ranges from 1 to -1 wherein -1 indicates that all ties are internal to the group and represents complete homophily in a network. An E-I index of +1 indicates that all ties are external to the group and would represent complete heterophily. A permutation test is combined with this index to evaluate the statistical significance of this measure by comparing the observed value to that of randomly generated values for networks of similar size and structure.

To answer RQ2, we further analyzed the network descriptives and network structure as mechanisms to compare the two networks (each having differing levels of technical expertise) to understand social patterns and features that differed between groups with low versus high levels of community collective efficacy. Fragmentation of the network is a whole network descriptors that can be used to note embeddedness of key players in the network. Fragmentation is an inverse measure of connectedness and refers to the proportion of mutually unreachable nodes in a network [7]. In exploring embeddeness of key players, we took a comparative approach using a specialized tool called Key Player, which is included with UCINET [8] that identifies key players in a network based on nodes which, when removed from a network, increase network fragmentation the most. These tools were used to identify individuals that are most embedded within the network. Once identified, we removed these nodes (i.e., individuals) from the network to assess how this affected the overall outcomes for community collective efficacy within each community. Using these varied analytical approaches, we viewed the social topography of the network from several perspectives. We present the key findings from our analysis in the results, which follow.

5 RESULTS

In this section, we first provide a contextualized description of the two older adult communities who participated in our survey and make comparisons between them. Then, we present our hypothesis testing based on our research framework, which addressed RQ1. To conclude our results, we answer RQ2 by examining the differing patterns between groups with lower and higher community collective-efficacy and identify group facilitators (e.g., employees and volunteers) as key players within the network.

5.1 Descriptive Characteristics of the Two Communities

Demographic information for both communities is provided in Table 1. In the sections below, we give a narrative description of these two communities.

5.1.1 Community 1: Retirement Community. The older adult community located in the Midwest (i.e., Community 1: "Residential") was a private residential assisted living community of 37 older adults and five employees. The residential retirement community was comprised of 37 older adults living at the facility, who participated in regular "happy hours," and 5 employees that supported these individuals on a daily basis. Reported interactions among the community are illustrated in Figure 2. As shown in Table 1, the average age of older adults in this community was 71 (SD = 4.2 years). Employees were younger in age than the residents, ranging from 39-65 (SD = 9.5 years), while the older adults were all 65 and older. The full community had an equal number of community members that identified as male (n = 21) and female (n = 21). The majority of the community had a college education (81%) and reported an annual household income of over $50,000 (98%) with 23 percent of the community reporting an annual household income of over $100,000. During visits to the residential community, it was clear that employees in this community had been trained to support residents' technical needs in order help them maintain connections with family members living outside of the community. This involved support with smartphones, tablets, laptops, and smart devices in resident living quarters.

5.1.2 Community 2: Social Community. The older adult community located in the Southeast (Community 2, "Social") were recruited from a government-run senior center community and consisted of a social group of friends (N = 22 older adults) and three community center volunteers. The social group participated in social and educational programming through instruction under a volunteer teacher. Participants were primarily recruited from a computing basics course that met at least twice a month, however, some individuals regularly participated in more classes

Table 1. Demographics of Residential (Res.) and Social (Soc.) communities with and without Employees and Volunteers.

	Total Res.	Total Soc.	Res.w/o Emp.	Soc.w/o Vol.	Res.Emp.	Soc.Vol.
N	42	25	37	22	5	3
Age (years)						
M	68.452	69.92	71.27	70.773	47.6	63.667
Md.	69	70	70	70	43	64
SD	9.217	4.175	4.202	3.68	9.457	1.247
Min.	39	62	65	63	39	62
Max.	80	78	80	78	65	65
Gender	*n* (%)	*n* (%)	*n* (%)	*n* (%)	*n* (%)	*n* (%)
Male	21 (50)	8 (32)	19 (51.4)	7 (31.8)	2 (40)	1 (33.3)
Female	21 (50)	17 (68)	18 (48.6)	15 (68.2)	3 (60)	2 (66.7)
Highest Ed.	*n* (%)	*n* (%)	*n* (%)	*n* (%)	*n* (%)	*n* (%)
Primary	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
Secondary	8 (19)	4 (16)	8 (21.6)	4 (18.2)	0 (0)	0 (0)
College	24 (57.1)	10 (40)	24 (64.9)	9 (40.9)	0 (0)	1 (33.3)
Masters	9 (21.4)	10 (40)	5 (13.5)	8 (36.4)	4 (80)	2 (66.7)
Doc./Prof.	1 (2.4)	1 (4)	0 (0)	1 (4.5)	1 (20)	0 (0)
Household Inc.	*n* (%)	*n* (%)	*n* (%)	*n* (%)	*n* (%)	*n* (%)
≤ $24,999	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
$25K–49,999	1 (2.4)	6 (24)	1 (2.7)	5 (22.7)	0 (0)	1 (33.3)
$50K–74,999	10 (23.8)	6 (24)	10 (27)	6 (27.3)	0 (0)	0 (0)
$75K–99,999	21 (50)	3 (12)	19 (51.4)	3 (13.6)	2 (40)	0 (0)
≥ $100K	10 (23.8)	6 (24)	7 (18.9)	5 (22.7)	3 (60)	1 (33.3)

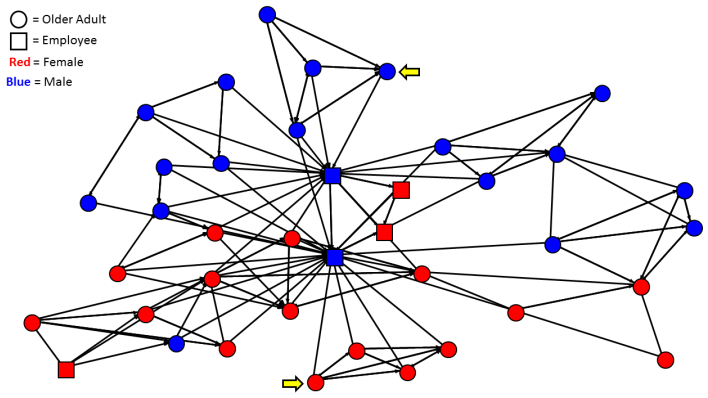

Fig. 2. Sociogram of Retirement Community. Note: Arrows highlight nodes noted in later results.

than others. In the computing basics course, volunteers help seniors 55 and older learn to use a laptop, tablet, iPhone or Android device; participants were asked to bring their own laptop

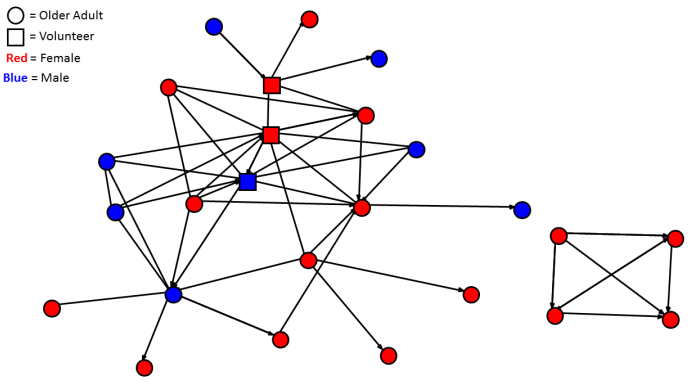

Fig. 3. Sociogram of Social Community.

computer or device, depending on the class focus. Although participants interacted with one another in class, Figure 3 highlights that some older adults only reported interactions with one other participant or a volunteer. As shown in Table 1, the average age of older adults in this community was 71 (SD = 3.7 years). Volunteers were more similar in age to older adults in the community, ranging from 62-65 (SD = 1.2 years), while the older adults were all 63 and older. The majority of members in this community identified as female (68%). The majority of the community had a college education (84%) and reported an annual household income of over $50,000 (76%) with 24 percent of the community reporting an annual household income of over $100,000. Although most survey participants completed all questions in the survey, four members of this community did not disclose their income range.

5.1.3 Comparing between the Two Communities. This section compares the two communities in terms of network descriptives and composite scores on each of the constructs using a t-test comparing means in each community.

In terms of network descriptives at the node level, the average degree of centrality in the residential network is 3.9, indicating that the average number of links that any individual has is 3.9 and the average degree of centrality of participants in the social group is 2. This is a directed network, meaning that a participant might list another as someone that they speak to regularly, but the other person might not list them in return. The number of incoming links that an individual has (i.e. the number of times that they are listed by other individuals in the community) is called in-degree centrality while the number of outgoing links (i.e. the number of times that others in the community list them) is called out-degree centrality. In- and out- degree centrality for each network are shown in Table 2. Whole network descriptives are described in subsection 5.3 to explore the embeddedness of key players within the network.

Next, Cronbach's alpha was used to ensure internal consistency of key constructs, as seen in Table 3 all scales were found to be highly reliable. Across each of the four constructs, there was a significant difference between mean scores among groups at $p<0.001$ as shown in Table 4. The social community reported mean scores of less than 2 on a 5-point Likert scale on each of the constructs, with the lowest value for community collective efficacy for privacy and security (M=1) and the highest for sense of community belonging (M=1.9). In contrast, across constructs, the residential community also reported the lowest mean value for community collective efficacy for privacy and security (M=2.4) and the highest scores for self-efficacy for privacy and security

Table 2. Degree Centrality by Community

Community	in-degree	out-degree
Residential with employees	*Md* = 3, *min.* = 0, *max.* = 29	*Md* = 4, *min.* = 2, *max.* = 5
Residential without employees	*Md* = 3, *min.* = 0, *max.* = 7	*Md* = 3, *min.* = 1, *max.* = 5
Social with employees	*Md* = 1, *min.* = 0, *max.* = 7	*Md* = 2, *min.* = 0, *max.* = 5
Social without employees	*Md* = .5, *min.* = 0, *max.* = 3	*Md* = 1, *min.* = 0, *max.* = 5

(*M*=3.4). This indicates that the social community rated individual and community capacity to manage privacy and security low, while the residential community perceived themselves to have moderate individual and community capacity to manage privacy and security.

Table 3. Internal consistency (Cronbach's Alpha) of key constructs.

Construct	No. Items	***M***	***SD***	***α***
Community Collective Efficacy	8	33.89	4.812	.922
Self-Efficacy	5	17.35	5.383	.971
Power Usage	22	77.68	18.192	.981
Sense of Community Belonging	7	26.09	5.970	.979

Note. α represents Cronbach's Alpha.

Table 4. T-Test comparing means of constructs in each community.

	Residential		Social		
	M	*SD*	*M*	*SD*	*t-test*
Collective Efficacy	2.4	0.70	1	0	13.2^{***}
Self-Efficacy	3.4	0.98	1.6	0.56	9.2^{***}
Power Usage	3.3	0.71	1.8	0.25	12.7^{***}
Community Belonging	2.5	0.51	1.9	0.25	6.7^{***}

Note. $^{***}p<0.001$

5.2 Hypothesis Testing Results

This section addresses each of the proposed hypotheses beginning with individual and community level factors that effect collective efficacy and then describes community level network effects.

5.2.1 Individual and Community Level Factors. To address RQ1, the results of the QAP correlation are shown in Table 5. As shown in Table 5, all of our constructs were significantly and positively associated with one another. This is to say, for example, that if an individuals' composite score for self-efficacy is low, their community collective efficacy is also likely to be low, likewise a high self-efficacy score is correlated with high community collective efficacy. Specifically, self-efficacy (H1a, r=0.734, p<.001), power usage (H1b, r=0.754, p<.001), and sense of community belonging (H1c, r=0.626, p<.001) were positively associated with community collective efficacy. Further, power usage was positively associated with self-efficacy (H2, r=0.591, p<.001). Therefore, H1 and H2 were both supported.

Demographic attributes of individuals are often posited as useful explanatory variables in statistical models, we included these in our correlation to examine differences in associations among constructs versus demographic categories. Although gender (r=0.06, p<.05) and income (r=0.16, p<.001) were both significantly and positively associated with community collective efficacy, these correlations were very weak and were not useful for explanatory purposes.

Table 5. Quadratic Assignment Procedure Correlation

Survey Scales							
	CCE	SE	PU	CB	G	E	I
Comm. Collective Efficacy (CCE)	1.00						
Self-Efficacy (SE)	0.73***	1.00					
Power Usage (PU)	0.75***	0.59***	1.00				
Sense of Community Belonging (CB)	0.63***	0.51***	0.57***	1.00			
Gender (G)	0.06*	0.05	0.12**	0.11**	1.00		
Education (E)	0.03	0.03	0.05*	0.06*	-0.02	1.00	
Income (I)	0.16***	0.09**	0.17***	0.13	-0.01*	0.08***	1.00

Note. *p<.05, **p<.01, ***p<.001

An additional community effect of interest to our analysis was sense of community belonging as a moderator of the relationship between self-efficacy and community collective efficacy, such that high levels of community belonging will strengthen the positive relationship between the two (H3). The QAP correlation shows correlations among all three, providing some evidence for this relationship, however, to adequately test the moderating effect, a sample with more variations in self-efficacy, collective efficacy, and community belonging would be necessary. In the case of our sample, groups reported similar scores among all three of these constructs. Despite inadequate data to uncover a statistically significant pattern, we observed two cases of participants in the residential community (see yellow arrows in Figure 2) where an individual indicated low self-efficacy but was connected to individuals with higher scores than themselves. Yet, these individuals reported high community belonging and indicated higher scores regarding community collective efficacy for privacy and security, despite their low scores for self-efficacy. An illustrative example of this is shown in Figure 4. Based on this anecdotal evidence, we conclude that hypothesis 3 is partially supported, but acknowledge that future work is needed to statistically confirm the validity of this potential moderating effect of community belonging.

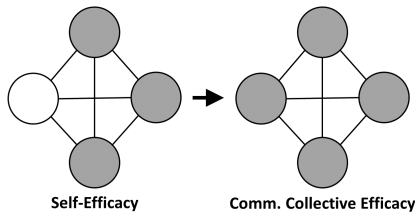

Fig. 4. Example of individual with low self-efficacy and higher community collective efficacy. Note: White = Low Score; Grey = Moderate Score.

5.2.2 Community-based Network Effects. To test H4, results of the E-I index to show tendencies towards homophily (i.e. network's preference for connections based on having the same attribute)

are shown in Table 6. Homophily for each of the scales in the framework had a significant E-I Index ($p<.05$) indicating that the number of times the random permutation test obtained a value greater than or equal to the observed and less than or equal to the observed was minimal. The E-I index is interpreted such that values closer to -1 represent a tendency towards homophily for a given attribute and values closer to +1 represent heterophily and a value closer to zero would indicate that there is not a tendency toward either. The test shows that there is a tendency towards homophily based on all constructs, in particular collective efficacy (-.456), power usage (-.485), and community belonging (-.529), although this tendency is less often the case for self-efficacy scores (-.221). There is also a tendency towards homophily based on gender (-.353) and heterophily based on education (.309) and income (.294), although only gender was found to be significant at ($p < 0.05$). Overall, E-I indices in Table 6 show that there is a tendency for participants to be connected with others with similar composite scores when it comes to community belonging, community collective efficacy, and power usage supporting hypothesis 4.

Table 6. E-I Index of variables.

Variable	E-I Index
Community Collective Efficacy	-.456
Self-Efficacy	-.221
Power Usage	-.485
Community Belonging	-.529
Gender	-0.353
Education	0.309
Income	0.294

5.3 Examining the Diffusion of Expertise through the Two Communities

The two networks we investigated differed in terms of size, mean scores on constructs, and number of average connections that each individual reported. The residential community was larger (see Table 1), reported higher mean scores on each of the constructs (see Table 4), and reported more connections to other members of the community (see Table 2).

Another key difference among communities is that they each had differing access to technology expertise through employees and volunteers. Evaluating whole network measures with and without employees and volunteers demonstrates that individuals in employee and volunteer roles play a key role in the social networks of older adults in these types of communities. Sociograms showing the distribution of collective efficacy in each community illustrates that the residential community contains employees embedded within the network with high collective efficacy. Older adults also share in levels of collective efficacy of those that that they are clustered with in small groups as seen in Figure 5. This sociogram confirms the importance of an individuals' connectedness within the community and connectedness with others who have a high community collective efficacy on their own community collective efficacy for privacy and security. In contrast, the volunteers in the social community are embedded, but have low collective efficacy as does the rest of the community, as seen in Figure 6. In this case, overall network cohesion of the community was not influential as the overall community collective efficacy was low. The following paragraph describes the embeddedness of employees and volunteers in each community and then compares the two.

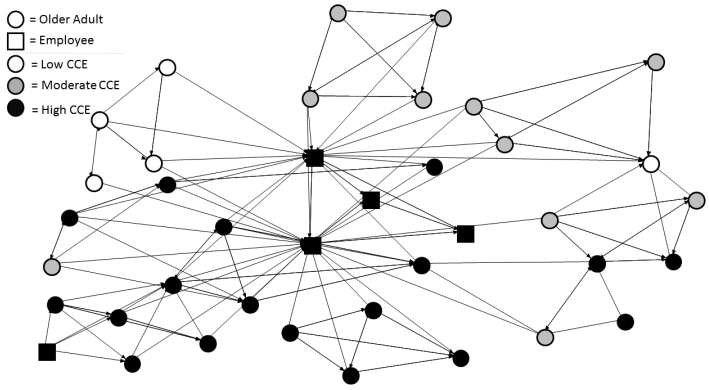

Fig. 5. Distribution of Community Collective Efficacy (CCE) in Residential Community.

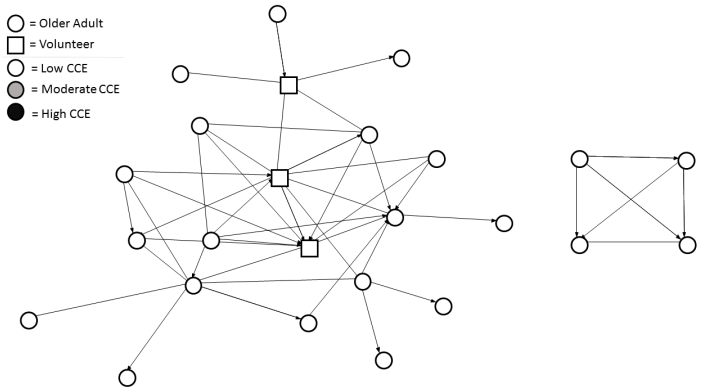

Fig. 6. Distribution of Community Collective Efficacy in Social Community.

The power usage scores of employees in the residential community were high among 4 of the 5 employees while the 3 volunteers in the social group had low scores in all four scales. In both groups, employees and volunteers were found to be key players, such that fragmentation in the network increases when removed. In the residential network shown in Figure 7, when employees are included (n = 42) the fragmentation of the network is 75%, indicating that the proportion of pairs of participants that are unreachable to one another is 75%. Fragmentation increases to 82% in the residential group when employees are removed. In the social community network shown in Figure 8, when volunteers are included (n = 25) the fragmentation of the network is 74% and the fragmentation increases to 95% when volunteers are removed.

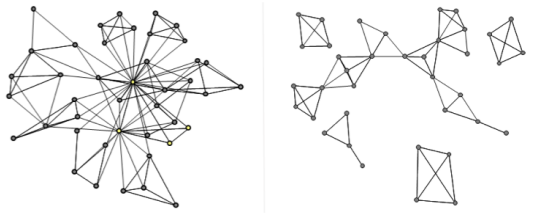

Fig. 7. Sociogram of residential community. Left: with employees; Right: without employees.

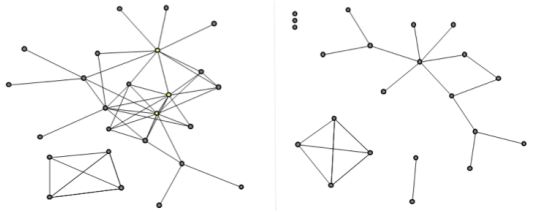

Fig. 8. Sociogram of Social Community. Left: with volunteers; Right: without volunteers.

As a result of these analyses, we have found evidence to support five of our six proposed hypotheses. A summary of all hypotheses and findings is shown in Table 7.

Table 7. Summary of hypotheses and findings.

Label	Hypothesis	Result
H1a	Self-efficacy for privacy and security will be positively associated with community collective efficacy for privacy and security.	Supported
H1b	Power usage will be positively associated with community collective efficacy for privacy and security.	Supported
H2	Power usage will be positively associated with one's self-efficacy for privacy and security.	Supported
H1c	Sense of community belonging will be positively associated with community collective efficacy for privacy and security.	Supported
H3	Sense of community belonging moderates the relationship between self-efficacy and community collective efficacy, such that high levels of community belonging will strengthen the positive relationship between the two.	Partially Supported
H4	Homophily will be present within communities based on demographic or construct similarity.	Supported

6 DISCUSSION

We conducted a social network analysis study to understand collective sense making and social support for digital privacy and security among older adults in two communities. This paper is the first work in digital privacy and security to introduce the concept of community efficacy. Thus, our approach was novel and contributes to our understanding of social cybersecurity, especially among a growing and understudied portion of the population. Community collective efficacy is a useful framework for examining privacy and security outside of typical usability research to improve design, and this paper provides a methodology for exploring community effects in more depth. Our work has the potential to influence future work on leveraging social support and community structures to support security and privacy learning. We demonstrate how communities of older adults may be able to support one another's privacy and security decision-making when technical knowledge is diffused throughout a community. In the discussion below, we identify the key implications of our findings for older adult communities and more broadly within the domain of digital privacy and security research.

6.1 Building Community Collective Efficacy for Privacy and Security within Older Adult Communities

Previous research has shown that individuals often rely on trusted others to make privacy and security decisions [21, 24, 53], but little research has investigated social environments that support increases in a personal capacity to address these issues. To address this limitation, we used community collective efficacy as a measure for examining the capacity for what Das calls social cybersecurity [20] and community oversight [15] in older adult communities. Our work is guided a framework of community oversight to better understand the individual- and community-level factors that support community collective efficacy for privacy and security. We first discuss this framework, and our related hypothesis before turning to implications of our results.

6.1.1 Individual-level factors. Recent studies have confirmed that while internet literacy has been increasing with the help of smartphones in recent years [28], there are still some older adults that have been slow to adopt [1] and are concerned about negative consequences relating to a lack of technical knowledge [39]. Therefore, we studied individual-level factors (i.e. self-efficacy and power usage) and how they correlated with community (i.e., sense of community belonging) and network-level factors (i.e., homophily) in the formation of community collective efficacy. Our findings affirm that results from related work on self-efficacy and community collective efficacy hold in the domain of privacy and security. A key implication of this finding is that individualized approaches of raising awareness and training older adults to manage their own digital privacy and security has the potential for enhancing the capacity for privacy and security decision making within the communities for which these individuals are embedded. Therefore, one possible strategy would be to identify key individuals within older adult communities, who have a high-level of centrality in the network, and invest time training those individuals on digital privacy and security. This would increase the probability that such knowledge would diffuse through the community.

6.1.2 Community-level factors. We also hypothesized, and confirmed, that sense of community belonging is related to community collective efficacy. A higher sense of belonging to a community is related to that group's perception of their ability to work together as a community towards privacy and security management. Thus, another intervention approach for enhancing community collective efficacy for digital privacy and security would be building stronger and more connected older adult communities. As we saw, the interconnectedness of Community 1 had a strong impact on the overall capacity of the community, whereas the looser ties in Community 2 seemed to

have the opposite effect. In a comparison of the social group and residential group, we found that overall, sense of belonging was lower in the social group than in the residential community. We also observed community collective efficacy for privacy and security to be lower in this group, however, self-efficacy and technology use were also much lower. The residential community that we surveyed contained many small self-selected groups of individuals that reported similar self- and community collective efficacy scores. There were only a few instances wherein one individual in a group reported lower self-efficacy than community collective efficacy for privacy and security. While building stronger communities and social connections seems counter-intuitive as an approach to improve privacy and security outcomes, our research builds the case that community oversight can do just that. Therefore, we make a call within the privacy research community to consider social factors and network effects when studying privacy and security. Understanding the extent to which this relationship holds will help determine what types of communities could provide support to each other, and whether strengthening community ties could also have a positive impact on collective privacy and security management.

6.1.3 Network Effects. Homophily was present within communities based on construct similarity (H4). There was remarkable similarity in constructs within the two communities. One explanation is that each of the communities attracted people with similar backgrounds and expertise. Another is that over time individuals learned from each other, resulting in similar perceptions of self- and community collective efficacy within these groups. In an investigation of the introduction of community expertise to support groups that have low community collective efficacy for privacy (RQ2) we compared each of the communities to one another with particular attention paid to key players in these communities. Examining measures of social cohesion (i.e. fragmentation) in these networks with and without employees demonstrated that employees were strongly embedded within the network. Taken together, these results lead us to believe that the technological expertise of individuals in these roles can have a large impact on communities of older adults and supports the notion that education and programming could support improved privacy and security management. We recommend that older adult programming aimed at online privacy and security be led by individuals who have relevant technological expertise in this area and feel confident in their personal capacity to manage devices.

6.1.4 Older Adults Supporting Each Other. Researchers are just beginning to examine how social factors and social support could influence users' privacy and security behaviors, and very little of this has focused on older adults. Yet, older adults could greatly benefit from help from others, and have already been shown to rely on friends and family for technology management [24]. Our results demonstrate that communities of older adult users could potentially provide this support to one another.

6.2 Implications for Digital Privacy and Security Research

This section describes the implications for this work for privacy and security research, including the use of community collective efficacy, and helping older adults to support one another through the distribution of technical expertise within these communities.

6.2.1 Studying Community Collective Efficacy for Privacy and Security. Our work is the first to propose and utilize a measure of community collective efficacy in the domain of privacy and security. According to Bandura [3], collective efficacy can influence how well groups use their resources, the effort they put forth, and commitment to overcome setbacks in trying to achieve goals. In this paper, we used this measure as part of understanding the dynamics of social networks that can benefit from social support. We confirmed that prior findings of the individual and community

factors that can enhance community collective efficacy hold with this population and in this domain. We believe the measure of community collective efficacy for privacy and security can be more widely used by researchers examining community-oriented behaviors and solutions for privacy and security management. Researchers could extend our results to further explore the factors that can enhance a group's ability to help each other. The relationship between users' individual and social support behaviors and community collective efficacy could also be investigated to provide additional guidance for how to support privacy and security management. Finally, researchers could examine the impact of technical interventions on community collective efficacy, as has been done in the domains of community informatics [13] and political participation [33].

6.2.2 Injecting Technical Expertise within Communities. A major finding of this work is that employees or volunteer that work within older adult communities may be an important facilitator of technological knowledge. In trying to increase the collective capacity of older adult communities, focusing on such employees could have strong impacts. A study of older adults' cybersecurity information-seeking behaviors by Nicholson et al. [50] found that older adults tend to prioritize social information resources based on availability, rather than cybersecurity expertise. Haney and Lutters [27] interviewed cybersecurity advocates and found that they must first establish trust with their audience and then empower them to adopt new practices. These prior findings may inform the design of training materials to be used by those that work with older adult populations. Thus, training with these employees on best practices for privacy and security may improve the overall community collective efficacy for privacy and security. Even in communities without such employees, focusing on other centralized and highly connected community members could have a similar impact.

6.3 Limitations and Future Research

We would like to identify some of the limitations of our research and suggest ways to address these limitations in future work. First, our sampling methods were limited to self-selected groups within two community groups and may not be generalizable to other populations of older adults. Future work should explore communities with broader demographics and socio-economic status [42]. Another limitation is that we examined perceived capacity to co-manage privacy and security rather than skills and expertise itself. Future work could examine more deeply the contexts of older adults that would support this form of social support, as well as the success of interventions in such communities.

A further limitation we experienced was due to the low between-person and between-group variance in our sample. Because of this lack of variance we only found two individual instances that gave partial support for H3, or the idea that individuals with a strong sense of community belonging can draw expertise from their community in a way that bolsters their collective efficacy for privacy and security. Given the potential implications of this finding, future work should collect data from a larger and more diverse sample of users to confirm if a moderating relationship exists.

While in this research we focused on communities entirely comprised of older adults, we need to further explore our framework and the social dynamics of other communities within which older adults are embedded. For example, older adults have many different social connections from where they could receive support, such as their families, friend groups, religious communities, and community organizations [24]. These groups may have more varied expertise and perspectives, which could impact the support they provide each other. We believe the framework we have examined and the methodology we have applied here will continue to be useful for exploring such communities.

Furthermore, it would be beneficial to expand our area of inquiry to other communities beyond older adults. While we explored older adults in this study, we believe that our framework would be useful to investigate a wide range of communities. Many users struggle with privacy and security management, have limited awareness of the risks, and limited knowledge of what to do to protect themselves. As several researchers have discussed, social support [20] or community oversight [15] mechanisms may help people work together to improve their privacy and security decision making. Thus, we believe our work could be extended to examine the social dynamics of other demographics, with different community structures, to determine which groups could best support each other in this domain and what kinds of interventions could improve users' collective abilities to manage security and privacy. Technology caregiving [59] is not a phenomenon that is unique to older adult communities as other community structures (e.g., families, co-workers, friends) may also benefit from shared community oversight [15] and the formation of community collective efficacy for privacy and security.

7 CONCLUSION

In this paper, we have examined the capacity of older adults to support each other in digital privacy and security management through the exploration of community collective efficacy. Our results highlight several factors that support community collective efficacy for privacy and security, namely individual self-efficacy for privacy and security, power usage of technology, and a sense of community belonging. Overall, our results indicate that each of the constructs examined plays a vital role in supporting community collective efficacy for privacy and security and warrants future work to understand other factors that may help communities that have low self-efficacy for privacy and security and low technology usage. One important contribution from this study is the important role that community facilitators can play in providing technical expertise in these communities, as we observed with the employees in the residential community.

Based on our findings, we believe our framework for building community collective efficacy may be useful to investigate individual- and community-based impacts when implementing privacy and security interventions. In addition, our social network analysis approach can aid in the examination of the socio-technical environment that may be critical to the success of such interventions, allowing researchers to focus on participant's relationships with others in their community. We contribute our work as an extension of the discussion on social cybersecurity and community oversight for privacy and security.

ACKNOWLEDGMENTS

We would like to thank the individuals who participated in our study. This research was supported by the U.S. National Science Foundation under grants CNS-1814068, CNS-1814110, and CNS-1814439. Any opinion, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the U.S. National Science Foundation.

REFERENCES

[1] Monica Anderson and Andrew Perrin. 2017. *Tech Adoption Climbs Among Older Adults.* Retrieved January 2, 2020 from https://www.pewresearch.org/internet/2017/05/17/tech-adoption-climbs-among-older-adults/

[2] Albert Bandura. 1982. Self-efficacy mechanism in human agency. *American psychologist* 37, 2 (1982), 122.

[3] Albert Bandura. 2000. Exercise of human agency through collective efficacy. *Current directions in psychological science* 9, 3 (2000), 75–78.

[4] Elizabeth Beck, Mary Ohmer, and Barbara Warner. 2012. Strategies for preventing neighborhood violence: Toward bringing collective efficacy into social work practice. *Journal of community practice* 20, 3 (2012), 225–240.

[5] Trevor Bennett, Katy Holloway, and David Farrington. 2008. The effectiveness of neighborhood watch. *Campbell systematic reviews* 4, 1 (2008), 1–46.

[6] Jeremy Birnholtz and McKenzie Jones-Rounds. 2010. Independence and Interaction: Understanding Seniors' Privacy and Awareness Needs for Aging in Place. Association for Computing Machinery, 143–152.

[7] SP Borgatti. 2003. Dynamic Social Network Modeling and Analysis: Workshop Summary and Papers, R. Breiger, K. Carley, P. Pattison, Eds. *National Academy of Sciences Press, Washington, DC* (2003).

[8] S.P. Borgatti, M. G. Everett, and L. C. Freeman. 2002. UCINET 6 for Windows: Software for Social Network Analysis. Harvard, MA, Analytic Technologies.

[9] Stephen P Borgatti, Martin G Everett, and Jeffrey C Johnson. 2018. *Analyzing social networks*. Sage.

[10] Kelly E. Caine, Celine Y. Zimmerman, Zachary Schall-Zimmerman, William R. Hazlewood, Alexander C. Sulgrove, L. Jean Camp, Katherine H. Connelly, Lesa L. Huber, and Kalpana Shankar. 2010. DigiSwitch: Design and Evaluation of a Device for Older Adults to Preserve Privacy While Monitoring Health at Home. In *Proceedings of the 1st ACM International Health Informatics Symposium*. Association for Computing Machinery, 153–162.

[11] Jason T Carbone and Stephen Edward McMillin. 2019. Neighborhood collective efficacy and collective action: The role of civic engagement. *Journal of community psychology* 47, 2 (2019), 311–326.

[12] John M Carroll and Debbie Denise Reese. 2003. Community collective efficacy: Structure and consequences of perceived capacities in the Blacksburg Electronic Village. In *36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the*. IEEE, 10–pp.

[13] John M Carroll, Mary Beth Rosson, and Jingying Zhou. 2005. Collective efficacy as a measure of community. In *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM, 1–10.

[14] Rajarshi Chakraborty, Claire Vishik, and H Raghav Rao. 2013. Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. *Decision Support Systems* 55, 4 (2013), 948–956.

[15] 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. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW (2019).

[16] Jane Chung, George Demiris, and Hilaire J Thompson. 2016. Ethical considerations regarding the use of smart home technologies for older adults: an integrative review. *Annual review of nursing research* 34, 1 (2016), 155–181.

[17] Lynne Coventry and Pam Briggs. 2016. Mobile technology for older adults: Protector, motivator or threat?. In *International Conference on Human Aspects of IT for the Aged Population*. Springer, 424–434.

[18] Sara J. Czaja, Neil Charness, Sankaran N. Nair, Wendy A. Rogers, and Joseph Sharit. 2006. Factors Predicting the Use of Technology: Findings From the Center for Research and Education on Aging and Technology Enhancement (CREATE). *Psychol Aging* (2006), 333–352.

[19] Sara J. Czaja, Chin Chin Lee, Sankaran N. Nair, and Joseph Sharit. 2008. Older Adults and Technology Adoption. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 52, 2 (2008), 139–143.

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

[21] 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.

[22] Sauvik Das, Adam DI Kramer, Laura A Dabbish, and Jason I Hong. 2015. The role of social influence in security feature adoption. In *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing*. ACM, 1416–1426.

[23] G. Demiris. 2009. Privacy and social implications of distinct sensing approaches to implementing smart homes for older adults. In *2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. 4311–4314.

[24] Paul Dourish and Ken Anderson. 2006. Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-computer interaction* 21, 3 (2006), 319–342.

[25] Rachel L. Franz, Leah Findlater, Barbara Barbosa Neves, and Jacob O. Wobbrock. 2019. Gender and Help Seeking by Older Adults When Learning New Technologies. In *The 21st International ACM SIGACCESS Conference on Computers and Accessibility*. Association for Computing Machinery, 136–142.

[26] 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)*.

[27] Julie M Haney and Wayne G Lutters. 2018. " It's Scary… It's Confusing… It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*. 411–425.

[28] SG Hong, S Trimi, and DW Kim. 2016. Smartphone use and internet literacy of senior citizens. *Journal of Assistive Technologies* 10, 1 (2016), 27–38.

[29] Dominik Hornung, Claudia Müller, Irina Shklovski, Timo Jakobi, and Volker Wulf. 2017. Navigating relationships and boundaries: Concerns around ICT-uptake for elderly people. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 7057–7069.

[30] Hsiao-Ying Huang and Masooda Bashir. 2018. Surfing safely: Examining older adults' online privacy protection behaviors. *Proceedings of the Association for Information Science and Technology* 55, 1 (2018), 188–197.

[31] Drina Intyaswati. 2017. The role of consumer privacy and security on brand loyalty. *Jurnal InterAct* 6, 2 (2017), 12–19.

[32] Andrea Kavanaugh, John M Carroll, Mary Beth Rosson, Than Than Zin, and Debbie Denise Reese. 2005. Community networks: Where offline communities meet online. *Journal of Computer-Mediated Communication* 10, 4 (2005), JCMC10417.

[33] Andrea Kavanaugh, B Joon Kim, Manuel A Perez-Quinones, Joseph Schmitz, and Philip Isenhour. 2008. Net gains in political participation: Secondary effects of Internet on community. *Information, Communication & Society* 11, 7 (2008), 933–963.

[34] Byoung Joon Kim. 2015. Political efficacy, community collective efficacy, trust and extroversion in the information society: Differences between online and offline civic/political activities. *Government Information Quarterly* 32, 1 (2015), 43–51.

[35] Florian Kirchbuchner, Tobias Grosse-Puppendahl, Matthias R Hastall, Martin Distler, and Arjan Kuijper. 2015. Ambient intelligence from senior citizens' perspectives: Understanding privacy concerns, technology acceptance, and expectations. In *European Conference on Ambient Intelligence*. Springer, 48–59.

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

[37] Bran Knowles and Vicki L. Hanson. 2018. The Wisdom of Older Technology (Non)Users. *Commun. ACM* 61 (Feb. 2018), 72–77.

[38] David Krackhardt and Robert N Stern. 1988. Informal networks and organizational crises: An experimental simulation. *Social psychology quarterly* (1988), 123–140.

[39] Sri Kurniawan. 2008. Older people and mobile phones: A multi-method investigation. *International Journal of Human-Computer Studies* 66, 12 (2008), 889–901.

[40] Edward O Laumann, Peter V Marsden, and David Prensky. 1989. The boundary specification problem in network analysis. *Research methods in social network analysis* 61 (1989), 87.

[41] Matthew L Lee and Anind K Dey. 2014. Real-time feedback for improving medication taking. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2259–2268.

[42] Mary Madden. 2017. Privacy, security, and digital inequality. *Data & Society* (2017).

[43] S. Marathe, S.S. Sundar, M. Nije Bijvank, H.C. van Vugt, and J. Veldhuis. 2007. Who are these power users anyway? Building a psychological profile. In *Proceedings 57th annual conference of the International Communication Association*. who.

[44] Marilyn Rose McGee-Lennon. 2008. Requirements engineering for home care technology. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1439–1442.

[45] 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.

[46] Miller McPherson, Lynn Smith-Lovin, and James M Cook. 2001. Birds of a feather: Homophily in social networks. *Annual review of sociology* 27, 1 (2001), 415–444.

[47] Tamir Mendel. 2019. Social Help: Developing Methods to Support Older Adults in Mobile Privacy and Security. In *Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers*. Association for Computing Machinery, New York, NY, USA, 383–387.

[48] George R Milne, James Beckman, and Marc L Taubman. 1996. Consumer attitudes toward privacy and direct marketing in Argentina. *Journal of Direct Marketing* 10, 1 (1996), 22–33.

[49] Tracy L Mitzner, Julie B Boron, Cara Bailey Fausset, Anne E Adams, Neil Charness, Sara J Czaja, Katinka Dijkstra, Arthur D Fisk, Wendy A Rogers, and Joseph Sharit. 2010. Older adults talk technology: Technology usage and attitudes. *Computers in human behavior* 26, 6 (2010), 1710–1721.

[50] 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.

[51] Brian O'Connell. n.d.. *Seniors: Victims of Identity Theft.* Retrieved January 2, 2020 from https://www.lifelock.com/learn-identity-theft-resources-seniors-victims-of-identity-theft.html

[52] Jessica M Perkins, Kristi S Multhaup, H Wesley Perkins, and Cole Barton. 2008. Self-efficacy and participation in physical and social activity among older adults in Spain and the United States. *The Gerontologist* 48, 1 (2008), 51–58.

[53] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. 2016. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 272–288.

[54] John Scott. 1988. Social network analysis. *Sociology* 22, 1 (1988), 109–127.

[55] Matthew Scult, Vivian Haime, Jolene Jacquart, Jonathan Takahashi, Barbara Moscowitz, Ann Webster, John W Denninger, and Darshan H Mehta. 2015. A healthy aging program for older adults: effects on self-efficacy and morale. *Advances in mind-body medicine* 29, 1 (2015), 26.

[56] Hu Shuijing and Jiang Tao. 2017. An Empirical Study on Digital Privacy Risk of Senior Citizens. In *2017 International Conference on Robots & Intelligent System (ICRIS)*. IEEE, 19–24.

[57] S Shyam Sundar and Sampada S Marathe. 2010. Personalization versus customization: The importance of agency, privacy, and power usage. *Human Communication Research* 36, 3 (2010), 298–322.

[58] Daphne Townsend, Frank Knoefel, and Rafik Goubran. 2011. Privacy versus autonomy: a tradeoff model for smart home monitoring technologies. In *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE, 4749–4752.

[59] Bill Van Parys. 2019. You don't need to be tech savvy to be a tech caregiver. https://www.fastcompany.com/90438110/you-dont-need-to-be-tech-savvy-to-be-a-tech-caregiver. (Accessed on 02/15/2020).

[60] Chien Wen Yuan, Jessica Kropczynski, Richard Wirth, Mary Beth Rosson, and John M. Carroll. 2017. Investigating Older Adults' Social Networks and Coproduction Activities for Health. In *Proceedings of the 11th EAI International Conference on Pervasive Computing Technologies for Healthcare*. Association for Computing Machinery, New York, NY, USA, 68–77.

A APPENDIX OF SURVEY SCALES

Survey items appear below in the order they appear in survey. All measures were adapted from pre-validated scales noted in text. Scales were measured on a 5-point Likert scale from 1 – Strongly Disagree. 2 – Somewhat Disagree. 3 – Neither Agree nor Disagree. 4 – Somewhat Agree. 5 – Strongly Agree.

A.1 Community Collective Efficacy for Privacy and Security

- Our community can cooperate to improve the quality of our decisions about online privacy and security.
- Despite other obligations, we can find time to discus our decisions about online privacy and security.
- As a community, we can handle the mistakes and setbacks resulting from our decisions about online privacy and security without getting discouraged.
- I am confident that we can be united in the decisions we make about online privacy and security that we present to outsiders.
- As a community we provide care and help for one another regarding our online privacy and security decisions.
- Our community can leverage outside resources and services for our members to ensure the quality of online privacy and security decisions.
- Our community can provide information for people with different interests and needs when it comes to online privacy and security decision-making.

A.2 Self-Efficacy in Privacy and Security

- I know that if I worked hard to learn about online privacy and security, I could make good decisions.
- Online privacy and security decision-making is not too complicated for me to understand.
- I think I am the kind of person who would learn to use best practices for good online privacy and security decision-making.
- I think I am capable of learning to help others make good online privacy and security decisions.
- Given a little time and training, I know I could learn about best practices for good online privacy and security decision-making for myself and my community.

A.3 Power Usage

- I love to use most technological gadgets like computers, smartphones, and other internet-enabled devices.
- I think most technological gadgets are complicated to use.
- I make good use of most of the features available in any technological device.
- I have to have the latest available upgrades of the technological devices that I use.
- Use of information technology has almost replaced my used of paper.
- I love exploring all the features that any technological gadget has to offer.
- I often find myself using many technological devices simultaneously (multitasking).
- I prefer to ask friends how to use any new technological gadget instead of trying to figure it out myself.
- In interfaces that I'm familiar with, I get frustrated each time I have to go through basic steps designed for new users.
- Using any technological devices comes easy to me.

- I feel like information technology is part of my daily life.
- I think smartphones that have multiple features like a camera, email, and apps are terrific.
- Using information technology improves my productivity.
- Using information technology gives me greater control over my work environment.
- Using information technology makes it easier to do my work.
- I like to challenge myself in figuring out how to use any new technology.
- A little bit of intuition is all that is needed to figure out how to use any new technology.
- I would feel lost without information technology.
- I need very detailed instructions when using any technological interface for the first time.
- On devices that I use often, I'm able to go to the particular area or link that is likely to provide me with relevant information without using the help feature.
- I like to learn new software or use new technological devices on my own.
- Many of my friends come to me to get help related to technological gadgets.

A.4 Community Belonging

- I can get what I need in this community.
- This community helps me fulfill my needs.
- I feel like a member of this community.
- I belong in this community.
- I have a say about what goes on in this community.
- People in this community are good at influencing each another.
- I feel connected to this community.
- I have a good bond with others in this community.