Growing Together for Digital Safety: Examining the Effects of Group Formation and Engagement in Building Privacy and Security Efficacy

JESS KROPCZYNSKI, University of Cincinnati, USA
MAMTAJ AKTER, New York Institute of Technology, USA
AMIR REZA ASADI, University of Cincinnati, USA
HANNA ALZUGHBI, Clemson University, USA
JINKYUNG KATIE PARK, Clemson University, USA
HEATHER RICHTER LIPFORD, University of North Carolina at Charlotte, USA
PAMELA J. WISNIEWSKI, International Computer Science Institute, USA

Understanding how social interactions affect privacy management is important in today's digital landscape. We are investigating collective management of privacy and security through a mobile application, CO-oPS, that allows people to view and discuss each other's app privacy settings within a community of users. Sixteen small, self-organized groups, totaling 81 participants, used the app over a four-week period. Data collection included pre- and post-study surveys measuring privacy perceptions (Community Belonging, Self-Efficacy, Community Collective Efficacy) along with in-app behavioral logs (messaging and viewing activity). In this paper, we present a social network analysis of our field study data, exploring the effects of group formation and engagement on building privacy and security efficacy through CO-oPS interactions. Our analysis reveals that while privacy perceptions were not initially homophilous, they grew more similar over time. Notably, proactively messaging others in the app enhanced personal privacy management confidence. Our results demonstrate the nuanced ways that groups can influence each other in addressing security and privacy needs.

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

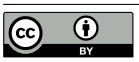
Additional Key Words and Phrases: Privacy and security, efficacy, collective privacy management, mobile application, social network analysis

ACM Reference Format:
Jess Kropczynski, Mamtaj Akter, Amir Reza Asadi, Hanna Alzughbi, Jinkyung Katie Park, Heather Richter Lipford, and Pamela J. Wisniewski. 2026. Growing Together for Digital Safety: Examining the Effects of Group Formation and Engagement in Building Privacy and Security Efficacy. *Proc. ACM Hum.-Comput. Interact.* 10, 2, Article CSCW018 (April 2026), 26 pages. https://doi.org/10.1145/3788054

1 Introduction

When interacting with digital technologies, individuals often lack the requisite knowledge and tools to effectively manage their data privacy [63]. At the same time, third-party applications frequently leak or misuse sensitive user data without obtaining informed consent [15, 52]. Although mobile

Authors' Contact Information: Jess Kropczynski, University of Cincinnati, Cincinnati, OH, USA, jess.kropczynski@uc.edu; Mamtaj Akter, New York Institute of Technology, New York, NY, USA, mamtaj.akter@nyit.edu; Amir Reza Asadi, University of Cincinnati, Cincinnati, OH, USA, asadiaa@mail.uc.edu; Hanna Alzughbi, Clemson University, Clemson, SC, USA, halzugh@clemson.edu; Jinkyung Katie Park, Clemson University, Clemson, SC, USA, jinkyup@clemson.edu; Heather Richter Lipford, University of North Carolina at Charlotte, Charlotte, North Carolina, USA, Heather.Lipford@charlotte.edu; Pamela J. Wisniewski, International Computer Science Institute, Berkeley, CA, USA, pwisniewski@icsi.berkeley.edu.



ACM 2573-0142/2026/4-ARTCSCW018
https://doi.org/10.1145/3788054

applications typically request permissions from users, these prompts are often laden with technical jargon, rendering them difficult for non-expert users to interpret accurately [30]. Moreover, certain third-party applications engage in deceptive practices by exploiting granted permissions to access additional personal information without explicit authorization [15].

Given this lack of transparency and comprehension, users often seek advice and guidance from their close social networks. Prior work has demonstrated that individuals commonly acquire privacy and security knowledge through informal storytelling [49] and discussions with family, friends, and colleagues regarding potential threats and protective strategies [24]. Users are more likely to trust and act upon privacy advice when it originates from trusted members of their social circles [53], and they are influenced to adopt privacy-preserving behaviors when these practices are modeled by peers within their networks [24, 44].

Motivated by these socially-driven dynamics, networked privacy researchers have called for community-based approaches to the co-management of digital privacy and security. For instance, AppMoD enabled users to delegate privacy-related decision-making to a trusted advisor within their network [64]. However, AppMoD primarily supported one-to-one delegation relationships. To extend this line of work, we developed CO-oPS ("Community Oversight for Privacy and Security"), a mobile application designed as an intervention platform to facilitate collective privacy and security management within trusted groups. CO-oPS enables community members to review each other's installed applications, examine granted or denied permissions, and communicate directly through in-app messaging to exchange feedback and guidance. We deployed CO-oPS among 16 groups of people who knew each other, where they engaged with the app over a four-week period and completed pre- and post-study surveys to evaluate changes in attitudes and behaviors. By employing a Social Network Analysis approach, our work provides actionable insights for designers and researchers in CSCW, particularly by demonstrating which specific in-app interaction patterns (e.g., proactive messaging) most effectively foster self-efficacy and collective agency in digital safety. This work supports moving beyond individual-centric solutions to architect more resilient, community-supported sociotechnical systems for privacy and security.

Thus, our research is driven by the following research questions:

RQ1: *How do demographic characteristics and privacy perceptions of individuals influence group dynamics when forming communities for collective privacy management?*

RQ2: *How do individual privacy perceptions change at the network level after participating in collective privacy management, and how are these perceptions interdependent?*

RQ3: *What collective privacy management activities positively influence individual privacy outcomes?*

This study employed a multi-faceted network analysis approach to investigate social dynamics and privacy-related factors within the online community. First, we explored how these different relational networks are structured by homophily, the tendency for individuals to connect with others who share similar characteristics (RQ1). We considered not only demographics but also key attitudes relevant in this context: community belonging [16], power usage [61], self-efficacy regarding privacy and security [6], and perceptions of the community's collective efficacy in ensuring privacy and security [17, 38]. We also examined the alignment between users' self-reported social connections and their actual in-app behaviors – direct messaging and viewing – actions that inherently involve active and passive interactions with others. Next, We tracked the evolution of these network structures and attitudes from before to after app usage (e.g. using pre- and post-surveys) (RQ2). Furthermore, we assessed the stability and interplay of these specific privacy-relevant attitudes. Finally, we aimed to identify whether and which engagement activities predict the outcome of using the CO-oPS app, namely an individual's gain in self efficacy and community collective efficacy (RQ3).

Our results reveal that who users reported knowing beforehand was significantly associated with their in-app interactions and viewing. This suggests that pre-existing social ties were reflected in both passive monitoring and active engagement online. The self-formed groups were highly similar across ethnicity. In stark contrast, connections based on attitudes toward community and privacy perceptions initially exhibited widespread heterophily, meaning that individuals tended to connect with others holding different attitudes at the study's outset. However, these attitudinal mixing patterns proved notably dynamic; they shifted significantly over the study period as attitudes tended to converge within groups. Actively reaching out to others via direct messaging was a significant predictor of gains in individual self-efficacy, suggesting a potential link between proactive communication and personal empowerment within this digital context.

The primary novel contribution of this research lies in its integrated examination of social network structures, dynamics of privacy-related perceptions, and distinct in-app behaviors within the unique context of an application specifically designed to facilitate collective engagement in privacy and security-preserving activities. While prior work might explore network effects of in-person interactions and general social media, or investigate privacy attitudes in isolation, this study distinctively bridges these domains. By situating this analysis within a mobile application explicitly designed to foster collective engagement in privacy and security-preserving practices, this study extends prior research by demonstrating how community-level digital safety initiatives can influence both individual and collective outcomes.

Specifically, our finding that proactive, outbound messaging is a significant predictor of individual self-efficacy gain offers the following design principle: systems must be engineered not just for information exchange, but to incentivize users to actively help and advise others. This moves privacy from a passive configuration task to an empowering, collective-action mechanism. Furthermore, the observed dynamic shift from attitudinal heterophily to alignment provides evidence of emerging, shared privacy norms within these groups, a key factor for the long-term success of community-based digital safety initiatives. Our findings offer valuable contributions to understanding how social dynamics interplay with individual and collective attitudes to shape engagement and potentially impact the success of technologies designed to foster community-based privacy and security practices. In addition, by demonstrating how network structures and attitudinal dynamics intersect to shape engagement in privacy and security practices, this study advances current conversations on sociotechnical systems, privacy management, and collective action. By demonstrating how these specific behavioral incentives and attitudinal dynamics shape engagement, this study advances current conversations on sociotechnical systems, privacy management, and collective action.

2 Background

2.1 Privacy and Security Management in Mobile Applications

The ubiquity of smartphone applications (apps) has introduced significant privacy and security challenges, as apps routinely access sensitive resources (e.g., location, contacts, health data) and may collect, store, or share this information in ways that users neither anticipate nor understand [62]. For instance, empirical studies of health-related apps demonstrate that many applications transmit personal health information without sufficient transparency, exposing users to potential data misuse and regulatory non-compliance [62, 69]. Moreover, analyses of mobile usage patterns reveal that users often exercise minimal caution regarding privacy in both public and private contexts, underestimate app-related threats, and comply readily with permission requests, further exacerbating risk [46].

Theoretical models have been applied to account for users' engagement in privacy-protective behaviors within mobile contexts. Protection Motivation Theory (PMT) suggests that elevated

perceived self-efficacy, vulnerability, and privacy concern motivate users to adopt risk-reducing behaviors, whereas greater awareness of app data practices can paradoxically diminish that motivation by increasing perceived response costs [68]. Complementarily, Communication Privacy Management theory frames privacy as the outcome of boundary negotiation between disclosure and control, highlighting the dynamic processes through which users manage information flow on mobile platforms [67]. To mitigate the well-documented privacy paradox, where users' stated concerns fail to align with their behaviors, personalized privacy notifications have been proposed to nudge users toward decisions that better reflect their expressed privacy preferences during app installation and permission grants [35].

Mobile operating systems employ permission models (e.g., Android's runtime permissions) to grant users control over app access to sensitive resources. However, expecting users to review and configure individual permissions for each installed app is often impractical, given the diversity of user preferences and the complexity of permission settings [41]. Prior studies indicate that while users exhibit consistent privacy and security preferences, they nonetheless struggle to locate and comprehend fine-grained settings without additional support [5].

To empower users in managing privacy and security, a range of sociotechnical interventions has been proposed. For instance, researchers have developed automated detection frameworks to identify privacy-harming behaviors in mobile apps [48]. The authors uncovered audio and video exfiltration without user consent and covert screenshot capture by third-party libraries, underscoring the need for real-time monitoring and mitigation strategies [48]. Privacy-aware recommender systems are leveraged to generate personalized suggestions that balance user burden and recommendation accuracy [60, 71]. In domain-specific contexts such as personal health, interactive mobile interfaces that demonstrate common security features—encryption, authentication, access control—have been shown to improve user comprehension and promote more informed privacy decisions [69].

Despite these advances, the multifaceted nature of privacy and security management in mobile applications demands integrated approaches that combine both individual empowerment and community engagement to support both personal and collective efficacy in safeguarding digital privacy. Therefore, beyond individual-level tools, a growing body of scholarship underscores the critical role of social capital and collective action in mitigating privacy risks, which we will explain in detail below.

2.2 Community-based Approaches for Privacy and Security

Beyond individual decision-making and isolated protective behaviors, a growing body of scholarship underscores the critical role of social capital and collective action in mitigating privacy risks [1, 2]. In particular, community-based models posit that trusted networks of peers—such as family members, friends, and co-workers—can collaboratively oversee and reinforce privacy hygiene, distributing knowledge and accountability across users [2]. For instance, empirical studies have demonstrated that extended family members often provide reciprocal technical support, with younger relatives guiding elders through security configurations and collectively negotiating app permissions, thereby reducing individual cognitive burden and enhancing overall digital safety [2]. Other research has explored privacy management within parent-teen relationships, shifting away from hierarchical parental control toward a cooperative framework in which all members engage in mutual monitoring and discussion of app permissions [3]. Such joint-family interactions not only alleviate tensions around surveillance but also promote collective learning and trust by situating privacy education within a supportive social environment [3]. Beyond familial structures, crowdsourcing frameworks gather community opinions on appropriate data sharing in different situations, helping to establish common guidelines for making privacy decisions [57].

Collaborative approaches to privacy and security management not only amplify user awareness by revealing prevalent privacy practices among peers but also address the critical issue of information trustworthiness. For example, prior work integrated expert user recommendations into crowdsourced frameworks to enhance the overall reliability of advice given to less experienced users. In this line of work, Rashidi et al. have proposed frameworks leveraging the insights of expert users, thereby enhancing the permission control process and ensuring that overall privacy and security practices are informed by qualified knowledge [51]. The power of social influences in shaping individual behaviors around privacy was further illustrated by studies conducted by Das et al. and Redmiles et al. that observed how social proof can encourage users to adopt specific privacy settings or security features based on observed behaviors of peers [24, 53]. Additionally, recent experiments by Mendel and Toch highlighted the inclination of individuals to favor advice from their close connections over established guidelines from community volunteers, revealing the strength of trusted relationships in guiding privacy behaviors [45].

Recognizing the communal aspect of privacy management, solutions like Wan et al.'s AppMoD empower users to delegate security decisions within their trusted networks, fostering a collaborative approach to app permissions [64]. Such community-centric strategies are vital in enhancing user agency and ensuring that mobile applications adhere to user-defined privacy standards. Taken together, these findings illuminate how community-based approaches, grounded in trust, reciprocity, and shared expertise, can complement technical safeguards to establish robust sociotechnical ecosystems for managing privacy and security in mobile contexts.

2.3 A Social Network Analysis Approach

Social Network Analysis (SNA) provides a powerful framework for examining how social structures, interpersonal ties, and shared attributes influence individual and collective behaviors in digital contexts [13]. By mapping interactions and identifying patterns of connection, SNA provides insights into how individuals and groups exchange information, form relationships, and exert influence in sociotechnical systems [43]. In the context of SNA, the most fundamental social unit is the dyad, representing the interaction between two individuals. These interactions, referred to as ties, serve as the basic building blocks of social networks [33]. SNA visualizations, or sociograms, depict individuals as nodes and their interactions as links, effectively mapping the social ties that form within a community [56]. By analyzing these connections, SNA reveals how relationships are structured and how information flows within a network. Another key concept in SNA is homophily, the tendency for individuals to connect with others who share similar characteristics, such as demographic attributes or privacy attitudes [40, 43], which helps explain why certain network structures emerge, as people are more likely to form connections with those they perceive as similar. In addition, SNA also enables the creation of network metrics that quantify the position and influence of nodes, such as centrality measures that identify key actors based on their connections, which offers analytical frameworks and visualization techniques that make social structures and interaction patterns more visible and interpretable [59].

Social Network Analysis has captured significant interest among both scholars and professionals across various fields [59], namely but not limited to education [31], sports [66], scientific discovery of physical problems [21], policy research [23], transportation [27], cyber security [39], and most importantly sociocultural studies [42], as it creates opportunities for framing social phenomena [4]. For instance, by applying SNA, researchers analyzed the patterns and structures of interactions on virtual communities such as email groups, chat rooms, and social networks, and provided insights into how individuals connect, share information, and form relationships online [42].

Despite its extensive application in various domains, its potential to examine privacy and security practices within community-based digital safety systems remains underexplored. As we live in a

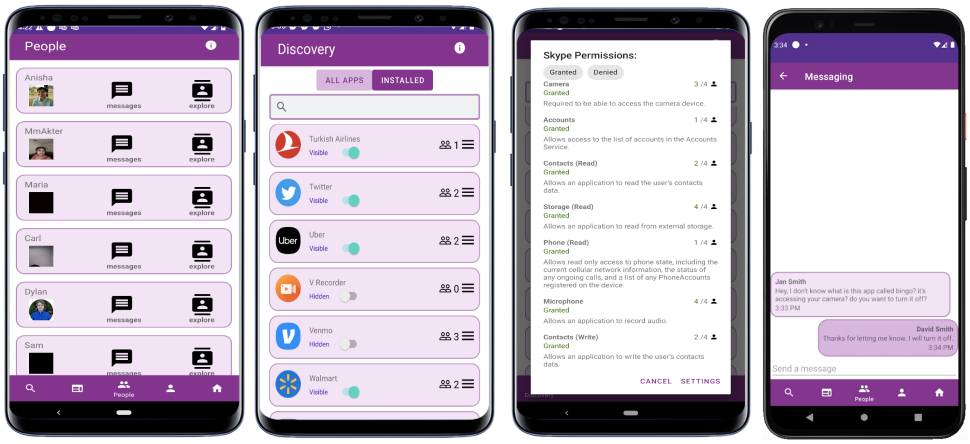
datafied society [32] where social, economic, and political relationships increasingly occur through digital mediums, the social architectures do not allow users to live in islands of privacy. Rather, as Gstrein and Beaulieu, Gstrein and Beaulieu argued, sharing the same time, space, and cultural dimension makes it difficult for an individual to stand apart. This context makes the usage of SNA relevant to study privacy, as it was used in previous studies [9, 19]. This study addresses this critical gap by leveraging SNA to examine how social connections in a community-oriented privacy management system influence privacy attitudes and efficacy.

Meanwhile, while SNA studies are highly reliant on the completeness of data, data is often incomplete, or does not include elements that represent the constructs researchers are investigating [55, 59]. This problem urges researchers to not just rely on individual data on public social networks, but also study community interactions using conventional data collection methods in social science, such as surveys, and interviews [59], as they provide significant data on social interactions[58].

We build upon prior this extensive prior literature by engaging with 81 participants in groups for a 4-week field study to examine how individual and collective factors, such as social network, impact their privacy practices on mobile applications. By integrating SNA with privacy management frameworks, this study contributes to the CSCW community by highlighting how network structures can be strategically leveraged to bolster both individual and collective privacy efficacy in mobile systems. This integrative approach provides a novel lens through which to understand how network structures and privacy attitudes intersect, offering design implications that extend beyond individual user behavior to encompass collective security and privacy practices.

3 CO-oPS App Design

We developed the Community Oversight of Privacy and Security (CO-oPS) Android application, based on the community oversight model introduced by Chouhan et al. [20], was designed with the core requirement of increasing user awareness and trust through community-sourced mechanisms that facilitate advice-sharing and active oversight among close relationships. The CO-oPS app enables users to form communities and engage in mutual oversight by reviewing one another's installed applications and associated permission settings. To support this collaborative approach,



(a) (b) (c) (d)

Fig. 1. CO-oPS App Interfaces: (a) People, (b) Discovery, (c) Permissions and (d) Messaging.

the app includes features for viewing apps and permissions and communicating through private, in-app messaging.

As illustrated in Figure 1a, the People Page provides users with a directory of their community members and access to the Discovery Page, where they can view the applications installed on each member's device. This feature facilitates transparency while also enabling private, in-app messaging, allowing users to exchange guidance and feedback on app installations and permission settings—thus promoting active participation in community-based privacy oversight. The Discovery Page (Figure 1b) allows users to explore the installed apps of any group member and access further details through the Permissions Page. This functionality is designed to enhance users' awareness of mobile privacy and security practices across the community. On the Permissions Page (Figure 1c), users can view their own permissions granted or denied for each app, as well as compare these settings with those of other members. A built-in shortcut to the device's system settings (via the "SETTINGS" icon) provides users with a convenient way to make changes directly. To balance transparency with personal privacy, CO-oPS also includes a feature that allows users to hide selected apps from their community. This empowers individuals to participate in shared oversight while maintaining control over their own privacy boundaries.

4 Methods

We recruited 16 small, self-organized groups, each consisting of 2 to 6 individuals who already knew one another. In total, 81 participants were enrolled, starting with initial contacts who then invited members of their social networks to join their group. Participants installed the CO-oPS Android app and used it over a four-week period to offer and receive feedback from each other within their group in making privacy-related decisions. Alongside the app usage, participants completed a survey both before and after the field study when they used the CO-oPS app. The study was reviewed and approved by the Institutional Review Boards (IRBs) at the participating universities.

4.1 Study Procedure

Each group first completed a pre-intervention survey which collected their demographic information and baseline measures of psychosocial factors relevant to privacy and security, namely Community Belonging, Self-Efficacy, and Community Collective Efficacy using 5-point Likert scales ranging from 1 (strongly disagree) to 5 (strongly agree). We also measured power usage—adapted from [61] by Sundar et al. — to capture participants' comfort with technology and their tendency to explore its features. The community belonging scale, based on [16] by Carroll, assessed how important individuals felt within their community and the extent to which they believed their opinions were valued. The self-efficacy scale [6], as defined by Kropczynski et al. in [38], measured participants' confidence in managing their own privacy and security. Community collective efficacy, also from Kropczynski et al. [38], gauges participants' perception of their community's ability to collaboratively address mobile privacy and security challenges. Participants were also asked to indicate their offline relationships with other members of their group, providing data on which members knew which other group members. During an intake survey, participants were asked to identify any other individuals in the study they already knew. This self-reported data was used to construct the initial social network map and define the pre-existing groups.

After completing the pre-survey, participants installed the CO-oPS Android app and used it within their respective groups for four weeks. Each week we sent a set of in-app tasks to our participants to suggest interaction with the app and their groups. These prompts were intentionally designed to stimulate sustained engagement throughout the four-week study period, thereby ensuring sufficient interaction data for analysis within the four-week study period. For example, Week 2 tasks prompted participants to: "From the "People" page, review one of your community

member's apps. Check if there are any apps or permissions that may not be safe. Send a message to warn them about unsafe apps or permissions." As the CO-OPS app functioned as the intervention platform in this study, these types of prompts represent a mechanism through which similar nudges could be embedded during actual use to guide and encourage positive privacy behaviors. During the field study, the CO-oPS app functioned as the intervention platform, enabling users to offer and receive privacy-related support and guidance. During this time, in-app behavioral data—including messaging activity and viewing logs—was collected. At the end of the intervention, participants completed a post-study survey that re-measured the same psychosocial constructs to assess changes over time, excluding power usage, as the app was not designed to improve general tech skills.

4.2 Social Network Data

Three distinct social networks among the final sample of 81 participants were constructed as NxN matrices – specialized data structures representing all possible pairs of individuals (dyads) and the state of the relationship or tie between them. The Self-Reported in-person (Survey) network, derived from pre-intervention survey responses and treated as undirected, represented pre-existing social ties. From the in-app behavioral logs, a directed Direct Messaging (Messaged) network was constructed representing who sent messages to whom (where the direction of the tie matters), and a directed Activity Viewing (Viewed) network represented who viewed whose activity feed or profile.

Participant attribute data were collected alongside network data. Demographic information on Age, Gender, Ethnicity, and Education level was obtained via the pre-intervention survey. Psychosocial attitudes were represented by composite scores derived from the validated scales-Community Belonging (CB), Self-Efficacy (SE), and Community Collective Efficacy (CCE). This approach was utilized to measure whether participants develop privacy management skills, and gained score in these aspects. Thus, change scores for Self-Efficacy (SEGain) and Community Collective Efficacy (CCEGain) were subsequently calculated as the difference between post- and pre-intervention scores (Post - Pre). Finally, standard network centrality measures – metrics quantifying an individual's position or prominence within the network structure – were calculated. Specifically, In-degree (representing the number of ties received by a node, e.g., messages received) and Out-degree (representing the number of ties initiated by a node, e.g., messages sent) were computed for each participant within both the Direct Messaging and Activity Viewing networks.

Prior to the main analyses, data cleaning procedures [10, 50, 70] were implemented to eliminate potential information irregularities [18] and to enable a more accurate identification of the phenomena occurring between individuals [36]. In-system activity log data were not successfully recorded for 7 of the originally enrolled 22 groups, necessitating their exclusion from analyses involving in-app network behaviors. Furthermore, 2 of the remaining 15 groups were subsequently excluded due to substantially incomplete survey data among some members, which would have compromised network integrity and attribute analyses. Consequently, the final dataset used for all reported analyses comprised 81 participants nested within 16 distinct groups.

4.3 Data Analysis Approach

Data analyses were performed using UCINET for Windows [11], incorporating methods specifically designed for the interdependent nature of network data. Unlike independent survey responses, network data points (like relationships) are often related (a property sometimes called network autocorrelation), requiring specialized statistical approaches.

To assess the alignment between different layers of social connection, the Quadratic Assignment Procedure (QAP) correlation was utilized. QAP is a specialized correlation technique that compares two entire networks dyad-by-dyad (comparing the state of the tie between the same pair of nodes in

both networks) to produce an overall correlation coefficient [12]. Significance is assessed through permutation tests, where the structure of one network is randomly shuffled thousands of times (while preserving basic properties) to see how often a correlation as strong as the observed one occurs merely by chance. QAP correlations were computed between the Survey network and the Messaged network, the Survey vs. Viewed network, and the Messaged vs. Viewed network.

Network structure concerning homophily – the principle that similar individuals tend to form ties with each other ('birds of a feather flock together') [43] – was examined using the E-I index (RQ1). This index quantifies the network's balance between ties formed within specified attribute groups versus ties formed between different groups, ranging from -1 (perfect homophily) to +1 (perfect heterophily, where ties predominantly form between dissimilar individuals). E-I indices were calculated for the Survey, Messaged, and Viewed networks based on demographic attributes and psychosocial attitudes. Continuous or Likert-scale variables, such as attitudes were split by standard deviations before E-I calculation for the whole network [37]. The dynamics of attitudinal mixing were explored by comparing E-I indices derived from pre-intervention attitude scores versus those derived from post-intervention scores.

Relationships between various participant attributes (RQ2), including demographics and attitudes, were investigated using QAP correlation procedures adapted, allowing for assessment of correlations between individual characteristics while statistically accounting for the network dependencies. The stability of attitudes was also assessed by correlating pre- and post-intervention scores using this method.

Finally, to understand predictors of attitude change (RQ3), node-level network regression analyses were conducted via Multiple Regression Quadratic Assignment Procedure (MRQAP) adapted for nodal outcomes [25]. These models predict individual-level outcomes (here, attitude gains) using predictors like network centrality measures, while statistically controlling for the network autocorrelation (non-independence) discussed earlier. Significance testing for the overall model and individual predictors relied on permutation tests (10,000 permutations), again using controlled network shuffling to provide robust p-values without relying on standard statistical assumptions potentially violated by network data. Separate models predicted SEGain and CCEGain from participants' in-degree and out-degree in the messaging and viewing networks. By employing validated scales, QAP, and MRQAP with permutation testing, our analytical approach ensures the statistical robustness and internal validity of findings against network autocorrelation, an important step for drawing reliable conclusions from interdependent social data.

4.4 Participant Recruitment and Demographics

We recruited a total of 81 participants, organized into 16 distinct groups. Recruitment was conducted through a combination of methods, including recruitment emails, phone calls, word of mouth, social media posts, and snowball sampling (where initial contacts invited members of their social networks). For each group, recruitment began with an initial contact person, who completed a screening survey to determine their eligibility. Eligibility criteria included the following: 1) reside in the United States, 2) are 13 years or older (the minimum age was set to 13 to align with the U.S. Children's Online Privacy Protection Act (COPPA) guidelines for online services and to include the perspectives of older adolescents, a key demographic for mobile technology use [28]), 3) have an Android smartphone, 4) are willing to install and use the CO-oPS app, and 5) can participate in this study with at least two other people they knew. The screening survey provided a brief overview of the study and the CO-oPS app. Eligible participants were then given a consent form, which explained the study's purpose: to assess how individuals within self-formed communities use the CO-oPS app to support one another in managing mobile privacy and security. After providing consent, participants were asked to share the screening survey with others they wished to invite

into their study group. Use of the app and data collection did not begin until at least 3 people in a group had downloaded and installed CO-oPS.

5 Results

This section begins with an overview of the primary network layers utilized in this study. Following the description and comparison of these datasets, we will present the findings from the analyses conducted to address each research question.

5.1 Descriptive Characteristics of the Network Layers

Table 1 summarizes the demographic characteristics of the total 81 participants who performed any activities (e.g; messaging or viewing) within the app, as well as the characteristics of the subsets of individuals who engaged with messaging (N=60) and with viewing (N=51). The overall participant pool was diverse in age but centered on young to middle adulthood, with the largest group aged 25-34 (44 participants, 54.3%), followed by those aged 18-24 (16 participants, 19.8%). This pattern was generally similar among those engaged in messaging and viewing. Males constituted the majority of the initial sample (50) and represented a slightly higher proportion among those involved in messaging (61.7%) and viewing (66.7%). Educational attainment was generally high, with Bachelors (37%) and Masters (40.7%) degrees being the most common qualifications in the initial sample; this trend towards higher education persisted in the app-engaged subsets, although the proportion with Masters degrees was higher among messagers (40.0%) while Bachelors degrees were more prevalent among viewers (45.1%). Ethnically, the sample was predominantly Asian (64 participants, 79%), with smaller proportions identifying as Black or African American (7.4%), White (3.7%), and Hispanic or Latino (9.9%). The strong representation of Asian participants (~75%) continued within the app-engaged groups, while Hispanic or Latino participants constituted a slightly larger percentage of those involved in messaging (13.3%) and viewing (15.7%) compared to the initial survey pool.

To compare group formation to in-app behaviors, we retained the 81 participants with recorded in-app activity for the analyses. Interactions representing group formation are considered on the network layer. This network layer maps self-reported knowledge ties derived from survey responses; this is the densest network, featuring 310 symmetric ties (meaning if A knew B, B also knew A), an average degree centrality of 3.83, and its largest connected group contains 6 individuals. In contrast, the second network layer representing in-app messaging network is sparser, comprising only 54 directed ties, yielding a much lower average degree of 0.67. The largest group linked by messaging involves 4 participants, and the network exhibits an arc reciprocity of 0.52, indicating that just over half of the messaging links were mutual. Similarly, the third network layer representing in-app viewing behavior is also directed, containing 72 ties with an average degree of 0.89. Its largest connected group consists of 5 individuals, and it shows slightly higher mutuality than messaging, with an arc reciprocity of 0.58.

Regarding the alignment between self-reported in-person relationships and in-app interactions, this study employed Quadratic Assignment Procedure (QAP) correlations. Specifically, we assessed how the network of reported in-person relationships (Survey) correlates with networks derived from direct messaging (Messaged) and activity viewing (Viewed) within the app. The analysis revealed significant positive associations across relevant network comparisons (refer to Table 2 for full results).

Specifically, the analysis showed a significant positive alignment between the network of self-reported in-person relationships (Survey) and the network representing who viewed whose activity within the app (Viewed) ($r = .315$, $p < .001$). This moderate correlation suggests that pre-existing social ties align with patterns of passive information consumption or monitoring within this digital environment.

Table 1. Participant Demographics Reported by Survey and Individuals Engaged in Mobile App.

Attribute	All Participants	App-Messaged	App-Viewed
N	81	60	51
Age (years)			
13 – 17	4	4	4
18 – 24	16	14	14
25 – 34	44	28	21
35 – 44	6	3	3
45 – 54	8	7	6
55 – 64	1	1	1
65+	2	2	2
Gender	*n* (%)	*n* (%)	*n* (%)
Male	50 (61.7)	37 (61.7)	34(66.7)
Female	31 (38.3)	23 (38.3)	17(33.3)
Highest Ed.	*n* (%)	*n* (%)	*n* (%)
Less than High Sch	5 (6.2)	5 (11.7)	5(11.8)
High School	1 (1.2)	1 (1.7)	1(2.0)
Some College	2 (2.5)	1 (1.7)	2(5.9)
Associate	3 (3.7)	2 (3.3)	1(2.0)
Bachelors	30 (37)	21 (35.0)	23(45.1)
Masters	33 (40.7)	24 (40.0)	14(27.5)
Doc./Prof.	7 (8.6)	4 (6.6)	3(5.9)
Ethnicity	*n* (%)	*n* (%)	*n* (%)
Asian	64 (79)	45 (75.0)	38(74.5)
Black or African	6 (7.4)	4 (6.7)	3(5.9)
White	3 (3.7)	3 (5.0)	2(3.9)
Hispanic or Latino	8 (9.9)	8 (13.3)	8(15.7)

Furthermore, a significant positive alignment was also found between reported in-person relationships (Survey) and active communication via direct messaging (Messaged) ($r = .338$, $p < .001$). This moderate correlation indicates that acknowledged in-person connections also align significantly with patterns of direct messaging within the app, suggesting that these broader social ties translate into this form of active engagement online.

Table 2. Quadratic Assignment Procedure (QAP) Correlations between three relations among participants.

	Survey	Messaged	Viewed
Survey	-		
Messaged	.338***	-	
Viewed	.315***	.431***	-

Note. ***p<0.001

Finally, a statistically significant link was also found between the two in-app behaviors – viewing activity (Viewed) and direct messaging (Messaged) ($r = .431$, $p < .001$), suggesting a notable tendency for these actions to co-occur.

Taken together, this demonstrates significant alignment between networks based on self-reported in-person relationships and networks derived from both types of in-app interactions studied. Specifically, acknowledged in-person ties showed moderate, significant positive correlations with both passive viewing ($r = .315$, $p < .001$) and active direct messaging ($r = .338$, $p < .001$) within the app. In other words, in-app messaging and viewing tended to occur between those in a group who already knew each other. The significant positive alignment suggests that the CO-OPS app successfully leveraged strong, pre-existing social capital to facilitate both passive monitoring and active guidance exchange, validating the study's premise that collective privacy management thrives on existing trust ties. Moreover, the two primary in-app behaviors themselves are moderately linked, indicating that passive observation and active communication are interconnected facets of engagement within this digital environment.

5.2 Network Homophily: Demographic Structure and Attitudinal Mixing

Table 3. Homophily: E-I Index of attributes across each participant relation (Survey, Messaged, Viewed).

	Demographic				Pre-Survey				Post-Survey			Gain	
	Age	Gdr.	Eth.	Ed.	PrCB	PrPU	PrSE	PrCCE	PstCB	PstSE	PstCE	SEGn	CCEGn
Srvy.	-0.25	-0.24	-0.88	0.12	0.29	0.23	0.37	0.39	0.33	-0.03	0.11	0.16	0.15
Mssg.	-0.41	-0.38	-0.86	-0.18	0.66	0.16	0.41	0.32	0.52	0.18	0.32	0.16	0.10
Vwd.	-0.06	-0.20	-0.83	0.14	0.44	0.20	0.36	0.49	0.37	-0.12	0.13	0.25	0.22

Variable abbreviations used in headers: Srvy. = Survey, Mssg. = Messaged, Vwd. = Viewed, Gdr. = Gender, Eth. = Ethnicity, Ed. = Education, Pr = Pre-Test, Pst = Post-Test, CB = Community Belonging, PU = Power Usage, SE = Self Efficacy, CCE = Community Collective Efficacy, Gn = Gain.

To understand how demographic characteristics and privacy perceptions shape group dynamics in collective privacy management (RQ1), our study analyzed homophily and heterophily patterns in group formation and subsequent in-app engagement. The E-I index was used to quantify the tendency for participants to associate with similar others (negative values), dissimilar others (positive values), or randomly mixing (values near zero). This index ranges from -1, indicating perfect homophily (ties exclusively between similar individuals), to +1, indicating perfect heterophily (ties exclusively between dissimilar individuals), with values around 0 suggesting random mixing. This allowed us to analyze how shared demographic traits and privacy beliefs shaped the structure of participant interactions within the groups through group formation and in-app behaviors (messaging and viewing).

Our analysis revealed that ethnicity was the strongest driver of initial group formation. Participants overwhelmingly reported knowing others of the same ethnicity within their groups, with a very strong homophily score (E-I = -0.884). This demographic pattern also influenced in-app engagement, as participants continued to view the activity of others from the same ethnic background (E-I = -0.827). Gender and age also shaped these social structures, though to a lesser degree. Gender-based homophily was moderate in both group formation (E-I = -0.239) and engagement (E-I = -0.197), while age-based homophily was more prominent during group formation (E-I = -0.252) but nearly absent during engagement (E-I = -0.056). Educational background showed a different pattern, with slight heterophily in both stages (group formation E-I = 0.123; engagement E-I = 0.139), suggesting that participants were somewhat more likely to connect across educational lines.

In contrast to demographic factors, initial in-app engagement was characterized by heterophily regarding privacy perceptions. At the beginning of the study, participants tended to view the activity of others who held different perceptions about community belonging (E-I = 0.438), personal confidence in managing digital privacy (self-efficacy; E-I = 0.358), and the group's collective ability to protect privacy (collective efficacy; E-I = 0.491). These patterns suggest that although participants formed groups based on demographic similarity, their early in-app interactions were more exploratory and exposed them to a broader range of privacy perceptions.

However, this diversity in privacy perceptions narrowed over time. As participants continued engaging with others in the app, they increasingly focused on individuals whose perceptions aligned with their own. Self-efficacy homophily shifted from moderate heterophily (E-I = 0.358) to slight homophily (E-I = -0.124), indicating a notable convergence towards individuals interacting with others who shared similar levels of confidence in managing their digital privacy. Collective efficacy showed a similar trend, with heterophily decreasing from 0.491 to 0.129, representing a substantial shift towards individuals engaging with peers who had similar perceptions of their group's collective ability to manage privacy. Community belonging also became more homophilous (E-I decreasing from 0.438 to 0.368). This represents a moderate shift towards individuals connecting with others who share similar perceptions of community belonging. These shifts indicate a dynamic process where initial demographic sorting gives way to a secondary sorting based on shared privacy perceptions as the community matures. This may reflect a process of seeking informational alignment or reinforcing existing beliefs through interaction with like-minded individuals, potentially influencing the effectiveness of collective privacy management within these groups.

Overall, the findings indicate that the initial formation of the group was driven largely by demographic similarity, particularly ethnicity, while early participation in the app enabled participants to connect with various perceptions of privacy. However, as participants continued to interact, their focus shifted toward more like-minded peers. This dynamic convergence strongly suggests that participants were not merely seeking similar peers, but were undergoing a process of social learning and negotiating shared privacy norms through interaction, transforming the group from a collection of individuals with diverse views into a community with emerging attitudinal coherence. This may reflect a natural progression in which participants, some of whom actively helped others with privacy decisions, began to develop a shared understanding or preference to engage with others who had similar perceptions and levels of digital confidence. These evolving patterns highlight how community dynamics can transition from exploratory to reinforcing, shaping the types of social learning and support that occur in systems designed for collective privacy management.

The takeaways from this analysis are:

- **Ethnicity strongly drives initial group formation:** People overwhelmingly preferred to group with and interact with others of the same ethnic background.
- **Other demographics play a smaller role:** Gender and age also led to some grouping with similar individuals, but to a lesser extent. Interestingly, people were slightly more open to connecting across different educational backgrounds.
- **Initial privacy interactions are diverse:** When first using the app, individuals tended to engage with others who had *different* views on privacy matters, such as their confidence in managing digital privacy or their sense of community belonging.
- **Over time, privacy views align:** As interactions continued, people increasingly focused on others who shared *similar* privacy perceptions, shifting away from the initial exploration of diverse viewpoints.

- **Group dynamics evolve:** Groups initially form around shared demographic traits (especially ethnicity) but then shift towards being shaped by shared perspectives on specific topics, like privacy, as community members interact more.

Table 4. QAP Correlations Between Pre- and Post-Test Variables and Gains

Variable	Pr-CB	Pr-SE	Pr-CCE	Pst-CB	Pst-SE	Pst-CCE	SE Gn	CCE Gn
Pr-CB	1.000	0.021	0.017	0.020	0.012	0.015	0.028	0.018
Pr-SE	0.021	1.000	0.058**	-0.006	0.144**	-0.005	0.052**	0.033
Pr-CCE	0.017	0.058**	1.000	0.027	0.021	0.120**	0.011	0.021
Pst-CB	0.020	-0.006	0.027	1.000	0.015	0.176**	-0.006	-0.010
Pst-SE	0.012	0.144**	0.021	0.015	1.000	0.027	-0.044*	0.006
Pst-CCE	0.015	-0.005	0.120**	0.176**	0.027	1.000	-0.012	-0.025
SE Gn	0.028	0.052**	0.011	-0.006	-0.044*	-0.012	1.000	0.134*
CCE Gn	0.018	0.033	0.021	-0.010	0.006	-0.025	0.134*	1.000

Note. * $p < 0.05$, ** $p < 0.01$.
Variable abbreviations used: Pr = Pre-Test, Pst = Post-Test, CB = Community Belonging, SE = Self Efficacy, CCE = Community Collective Efficacy, Gn = Gain.

5.3 Attribute Intercorrelations and Network-Level Changes in Privacy Perceptions

To investigate how individual privacy perceptions evolved at the network level after participation in collective privacy management, and the interdependencies of these perceptions (RQ2), we employed QAP correlation analysis, accounting for network dependencies. Table 4 presents the correlations between pre-test and post-test attitudes/behaviors, and the gains observed within the networked groups. The results offer insights into the stability of these perceptions and how changes in one related to changes in others over the study period. We observed modest but significant stability in Self Efficacy (r=.144**) and Community Collective Efficacy (r=.120**) from the beginning to the end of the study. In contrast, Community Belonging showed no significant temporal correlation (r=.020), indicating that a participant's initial sense of belonging was not a predictor of their sense of belonging at the end of the study.

The analysis consistently pointed to an interconnectedness between individual and collective efficacy perceptions. At the beginning of the study, the self-efficacy (SE) and the community collective efficacy (CCE) were weakly yet significantly positively correlated (r=.058**). This relationship strengthened over time, as evidenced by a moderate positive correlation between Post-Test Community Belonging (CB) and Post-Test CCE (r=.176**). Importantly, changes in these efficacy beliefs were also linked at the network level. Self Efficacy Gain and CCE Gain showed a significant positive correlation (r=.134*), indicating that participants who experienced a greater increase in their personal confidence in managing privacy also tended to be in groups where the perceived collective ability to manage privacy increased. Interestingly, a higher initial self-efficacy was weakly associated with slightly higher individual gains in self-efficacy (r = 0.052 **), a finding that warrants further exploration in the context of network influence.

Figure 2 visually represents the groups that experienced an increase in Community Collective Efficacy (CCE). The sociograms illustrate the network of interactions within these groups, with nodes colored by high (green) and low (red) levels of SE, CB, and CCE, and arrows indicating the direction of interaction. The overall trend within these seven groups suggests that an increase in CCE often coincided with a general increase in SE within the group, supporting the positive

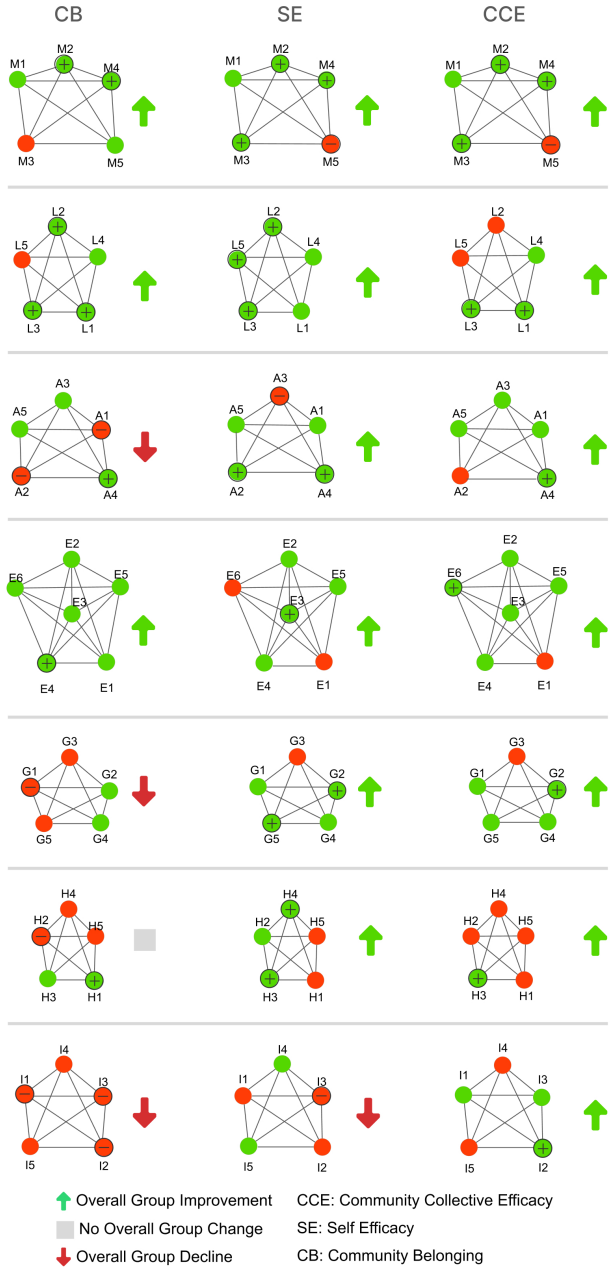


Fig. 2. Group sociograms illustrating CCE increase. Nodes represent individual participants, labeled with anonymized IDs (e.g., M2, G1). Letters (A-Z) denote distinct social groups that were identified based on pre-existing connections reported by participants during the intake survey.

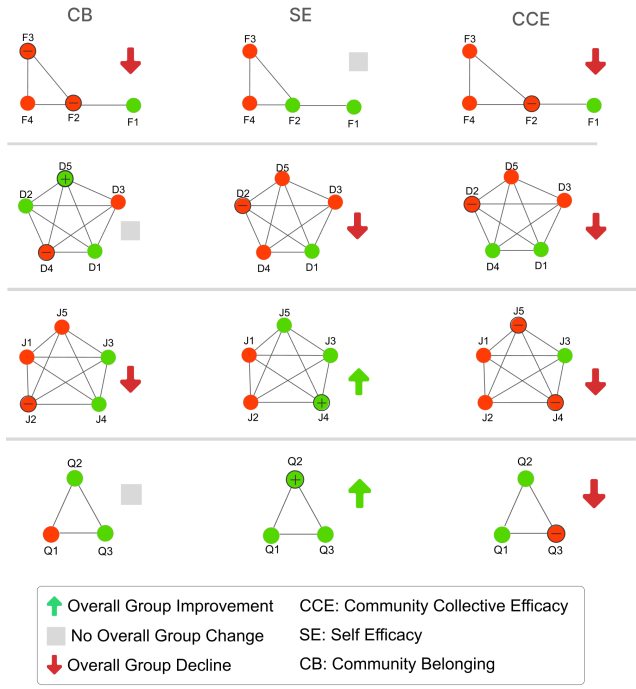


Fig. 3. Group sociograms illustrating CCE decrease. Nodes represent individual participants, labeled with anonymized IDs (e.g., M2, G1). Letters (A-Z) denote distinct social groups that were identified based on pre-existing connections reported by participants during the intake survey.

correlation observed in the QAP analysis. Furthermore, the groups with the most substantial CCE gains also tended to exhibit higher levels of CB, hinting at a supportive network environment fostering both individual and collective empowerment. The individual-level trends within these groups further reinforce the link between increased CCE and positive changes in both CB and SE. Notably, CCE increase appeared more common in larger groups, potentially indicating that a larger network provides more opportunities for shared learning and reinforcement of collective efficacy beliefs.

Figure 3 depicts the four groups that experienced a net decrease in CCE. These sociograms suggest that smaller groups, or larger groups characterized by members with persistently low CB and SE who did not show improvement, were more susceptible to a decline in perceived collective efficacy. This observation aligns with the network-level correlations, suggesting that a lack of individual empowerment and strong community bonds within a network may hinder the maintenance or growth of collective efficacy beliefs. The visual representation underscores the potential interdependence of individual privacy perceptions and the overall sense of collective agency within the network.

This analysis showed:

- **Some privacy feelings are more stable than others:** People's confidence in their own ability to manage privacy (Self Efficacy) and their belief in the group's ability to protect privacy (Community Collective Efficacy or CCE) stayed somewhat consistent from the beginning to the end of the study. However, their sense of belonging to the community varied more.

- **Personal and group confidence are linked:** Individuals who felt more confident about their own privacy skills also tended to be in groups that felt more confident about their collective privacy skills. This connection even grew stronger over time.
- **Gains in confidence go together:** When individuals experienced a boost in their personal confidence about managing privacy, the group they were in also tended to show an increase in its perceived collective ability to manage privacy.
- **Supportive groups see better collective outcomes:** Groups where the overall belief in their collective privacy strength (CCE) increased often had members who also felt more personally confident and had a stronger sense of community belonging.
- **Larger groups might foster more collective confidence:** An increase in the group's perceived ability to manage privacy (CCE) seemed to happen more often in larger groups.
- **Low individual confidence can bring down group confidence:** Groups that saw a decrease in their collective ability to manage privacy were often smaller, or had members with consistently low feelings of personal confidence and community belonging.

5.4 Predicting Individual Privacy Outcomes: Node-Level Regression

Table 5. Summary of Network Regression Analysis Predicting Self-Efficacy Gain (SEGain) (N = 81 Nodes)

Predictor	*B*	*SE*	β	*t*	*p*
Constant	0.466	0.107		4.355	-
Out-Degree Messaging	0.362	0.127	0.381	2.859	.007**
In-Degree Messaging	-0.154	0.112	-0.183	-1.374	0.172
Out-Degree Viewing	-0.118	0.08	-0.212	-1.473	0.139
In-Degree Viewing	-0.031	0.092	-0.049	-0.34	0.735

Note. Regression analysis accounts for network non-independence using permutation tests (10,000 permutations), via Multiple Regression Quadratic Assignment Procedure (MRQAP) adapted for nodal outcomes. N = 81 nodes. R^2 = .124, Adj. R^2 = .078. Overall model significance based on permutations approximates $F(4, 76) = 2.692$, $p = .039$. Individual predictor p-values are 2-tailed, based on permutations. *SE* = Standard Error estimated via permutation. t-statistics are provided for reference but significance is determined by permutation p-values. Significance for the Constant is typically not assessed via permutation.

To understand how collective privacy management activities within the app influenced individual privacy outcomes (RQ3), we investigated the relationship between participants' messaging and information-viewing behaviors and their gains in self-efficacy. We conducted a network regression analysis (MRQAP adapted for nodal outcomes) to predict individual Self-Efficacy Gain (SEGain) based on participants' positions within the messaging and viewing networks (N = 81 nodes), controlling for network dependencies through permutation tests (10,000 permutations). Predictors included participants' out-degree (sending messages and viewing others) and in-degree (receiving messages and being viewed).

The overall regression model was statistically significant (R^2 = .124, Adjusted R^2 = .078, approximated $F(4, 76) = 2.692$, $p = .039$ based on permutations), indicating that participants' patterns of interaction within the CO-oPS app were associated with changes in their individual confidence in managing digital privacy.

Specifically, Out-Degree in the Messaging network emerged as a significant positive predictor of SEGain ($\beta = 0.381$, $SE = 0.127$, p = .007). This finding suggests that individuals who actively reached out and initiated messages with a larger number of distinct peers within the app experienced greater increases in their self-efficacy regarding privacy management. In contrast, receiving messages

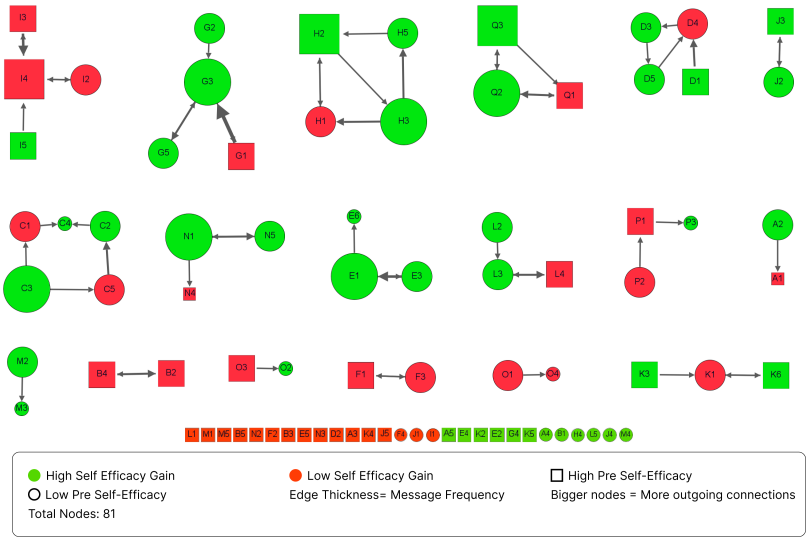


Fig. 4. Sociogram of SE Gain

(In-Degree Messaging: β = -0.183, p = .172) and both initiating and receiving viewing activity (Out-Degree Viewing: β = -0.212, p = .139; In-Degree Viewing: β = -0.049, p = .735), and In-Degree Viewing (β = -0.049, p = .735) were not significant predictors of individual self-efficacy gains in this model. Table 5 provides the detailed results of this analysis.

Figure 4, a sociogram visualizing the messaging network colored by SE Gain, further illustrates this finding. Participants who sent messages to more others (larger nodes) tended to exhibit higher SE Gain (green nodes). This suggests that actively engaging in direct communication and sharing information or support with a broader set of peers within the community was a key collective privacy management activity associated with positive individual privacy outcomes, specifically increased self-efficacy This result implies that the act of proactively offering advice or initiating help (out-degree) is a greater source of personal mastery and efficacy gain than simply receiving assistance or passively monitoring peers. This validates the self-efficacy theory principle that performance accomplishments—like successfully advising others—are key drivers of competence in a digital safety context.

Interestingly, parallel analyses examining the prediction of Community Collective Efficacy Gain (CCEGain) using the same network measures yielded no significant results. This suggests that while individual self-efficacy was influenced by active participation in direct communication, the collective perception of the group's ability to manage privacy was not significantly predicted by these specific network position measures. This highlights a potential distinction between the individual benefits of active engagement and the factors that contribute to a group's overall sense of collective efficacy. This distinction highlights that while individual proactive effort directly enhances personal confidence (Self-Efficacy), the development of a shared belief in the group's ability (Collective Efficacy) is likely dependent on broader factors beyond simple interaction frequency, such as successful group-level problem resolution or perceived competence of the group as a whole.

Based on this analysis, we found:

- **Actively messaging more people boosts individual privacy confidence:** Individuals who sent messages to a wider range of different peers in the app experienced a greater increase in their personal confidence about managing their digital privacy.
- **Other interactions didn't show the same benefit for individual confidence:** Simply receiving messages, viewing others' activity, or having one's own activity viewed did not significantly predict an increase in an individual's confidence in managing their privacy.
- **Individual confidence gains differ from group confidence:** While sending messages helped individuals feel more confident, these specific network activities (like how many people someone messaged or viewed) did not significantly predict changes in the group's overall collective confidence in its ability to manage privacy.

6 Discussion

6.1 Demographic Homophily and the Evolution of Attitudinal Alignment

In addressing the question of how demographic characteristics and privacy perceptions influence group dynamics in collective privacy management (RQ1), our findings reveal a two-stage process. Initial group formation, as reflected in the self-reported networks, was strongly shaped by demographic homophily, with ethnicity emerging as the most significant factor. Participants overwhelmingly reported pre-existing ties with others of similar backgrounds. This aligns with social identity theory and self-categorization theory, well documented in literature on online community formation, wherein individuals favor ingroup members in establishing social bonds in online spaces [26, 54]. This characteristic homogeneity of our study population, particularly regarding ethnicity, provides a valuable case study for understanding how strong pre-existing demographic ties can influence initial engagement and subsequent social dynamics in collective privacy management. Gender and age also contributed to homophily, albeit to a lesser degree, while educational background showed a slight tendency towards heterophily, which may indicate seeking of diverse perspectives, a dynamic sometimes explored in research on collaborative learning. This dynamic may also reflect prior work in collective privacy management involving extended family members, such as adults and teens, whose co-management reflected prior care-giving relationships [1, 2]. While this study did not directly analyze the correlation between specific app privacy settings and demographic factors, our findings on demographic homophily in interaction patterns suggest that social ties formed along these lines could indirectly influence shared privacy practices.

Within the context of in-app engagement, while ethnic homophily persisted in both messaging and viewing in-app behaviors, the early states of interaction were characterized by heterophily regarding privacy-related attitudes such as community belonging, self-efficacy, and collective efficacy. Participants initially tended to engage with others holding diverse privacy perceptions, suggesting uncertainty at the group formation phase. Over time interacting in the app, this pattern evolved toward greater alignment of privacy perceptions among interacting individuals, with a lesser degree in heterophily and, in some cases, a trend toward slight homophily. This convergence could be interpreted through the lens of developing shared mental models or common ground, concepts known to set the foundation for effective online collaboration [29]. The increasing attitudinal homophily might also reflect that individuals with similar privacy concerns or management approaches gravitate toward each other for support within the community of collective privacy management.

6.2 Collective Privacy Management and Transformation of Individual Privacy Perception

Regarding RQ2, which explores changes in individual privacy perceptions at the network level after collective privacy management, our findings reveal interdependent development of privacy efficacy. While supportive communities demonstrated significant potential as incubators for privacy self-efficacy, the development of both individual and collective efficacy perceptions are contingent on the nature and density of network interactions. The principle that efficacy flourishes within a "rich tapestry of interconnections" aligns with literature emphasizing how dense and diverse communication facilitates shared understanding, trust, and collective action [34]. When this communication is sparse or individuals become isolated, as observed in some groups, the positive effects on privacy perceptions diminish, suggesting that mere participation is insufficient without active network engagement.

The decline in community collective efficacy (CCE) observed in four smaller groups (2-3 members), compared to growth in groups with four or more members highlights how network structure and size can critically moderate outcomes. Insufficient group size may limit the diversity of inputs and the opportunities for vicarious learning or verbal persuasion, which Bandura [7] identifies as important sources of self-efficacy that can aggregate toward CCE. The isolation of members like J4, J5, D2, and F2 (see Figure 3), left them without social reinforcements, leading to a predictable decline in their CCE. This underscores how network position can directly impact individual outcomes, preventing the necessary social feedback loops that build and sustain collective beliefs [14]. Furthermore the decline in community belonging for some, echoing Carroll's [16] findings on the CCE-community bond correlation, suggest that a weakened sense of group cohesion directly undermines belief in the group's collective capabilities. These instances point to an interdependence where individual perceptions are shaped by their integration within a group communication network, and the collective perception (CCE) is the emergent property based on the quality and quantity of these interactions as well as the overall group cohesion.

6.3 The Role of Proactive Communication in Self-Efficacy Gain

Addressing the third research question concerning the influence of collective privacy management activities on individual privacy outcomes (RQ3), our analysis revealed a significant relationship between participants' active engagement in direct messaging and their individual gains in self-efficacy. Specifically, out-degree centrality in their messaging network (representing the number of people a participant messaged in the app) positively predicted increases in self-efficacy regarding privacy management. This aligns with prior research on knowledge sharing and the empowering effects of providing assistance in online communities. By actively interacting with other participants and engaging in activities like offering advice and articulating their own methods of privacy management, they engage in activities that have been shown to enhance self-efficacy and sense of expertise [8].

Expanding on this, it is interesting to note that the findings show that the number of messages someone sends can boost their own sense of self-efficacy, but it does not always translate into feeling more confident in the group's abilities (CCE). Messaging out-degree reflects an individual's proactive efforts to engage with others. This engagement can foster individual self-efficacy through mechanisms outlined in Bandura's theory of self-efficacy [7]. When individuals reach out to others for information on privacy management and successfully understand it, they experience performance accomplishments, enhancing their self-efficacy by proving that they can find solutions. Additionally, expressing their thoughts and strategies about privacy helps organize their understanding, further boosting their sense of competence. Lastly, positive feedback from peers,

such as validating concerns or praising strategies, serves as verbal persuasion, reinforcing belief in their abilities.

The link between messaging out-degree and increased self-efficacy is theoretically consistent with Bandura's work, and further the findings resonate with literature on network centrality, where individuals in more active or central positions often gain individual benefits like enhanced learning or influence due to increased information flow and opportunities for interaction [14, 65].

This insight holds significant practical utility for developers and policy-makers. By focusing design efforts on facilitating and rewarding proactive help-giving (i.e., outgoing advice), platforms can transition from being tools to becoming social catalysts for digital empowerment. The usefulness of this work is therefore in providing a clear, measurable interaction metric (messaging out-degree) that directly correlates with a positive individual outcome (SE gain), guiding where limited design resources can be prioritized.

6.4 Design Implications

Based on our analysis of social dynamics and efficacy gains, we offer two core actionable recommendations for CSCW researchers and system designers building future tools for data security: First, design must prioritize Proactive Empowerment, engineering digital safety interfaces to incentivize and reward active help-giving (out-degree interactions) as the primary mechanism for increasing individual self-efficacy, recognizing that the act of supporting others is the greatest source of personal mastery [8]. Second, systems must design for Attitudinal Cohesion, facilitating the negotiation of shared privacy norms by supporting the community's natural progression from diverse attitudinal mixing toward intentional alignment, ensuring that the collective system actively reinforces consensus on digital safety practices [29]. In the following paragraphs, we detail specific design implications derived from our findings that support these two principles, moving from generic, one-size-fits-all privacy warnings to systems that harness verified social dynamics for effective intervention.

Leverage pre-existing social connections to boost engagement. Harnessing pre-existing social ties is important achieving initial user engagement and sustained collective management, laying the groundwork for both proactive empowerment and attitudinal cohesion. The observed alignment between self-reported acquaintanceship and in-app messaging and viewing behaviors suggests that leveraging existing social ties can be critical in seeding initial user engagement, which is the first key step toward sustained collective management. Design features that facilitate connecting with known contacts within the app (e.g., friend suggestions, contact imports) can facilitate these connections. Additionally, enabling users to seamlessly transition from viewing content to initiating direct messages can further support social interaction and sustained participation while adhering to contextual norms that govern messaging behaviors within established networks [47]. Furthermore, our paper shows that privacy and security expertise within the network is a prerequisite for collaborative approaches to benefit the wider community, asserting that CSCW researchers must invest more time researching how to infuse such expertise to amplify broader network effects.

Encouraging proactive communication to enhance individual self-efficacy. The positive association between messaging out-degree and self-efficacy gains underscores the value of proactive communication. Given that the CO-OPS app served as an intervention, the effectiveness of weekly prompts in stimulating engagement highlights how similar prompts can be embedded during actual use as a way to nudge user behavior in positive privacy directions. Hence, designers can consider features that encourage users to initiate interactions, such as prompts to share privacy tips or discussion starters. Gamified elements that reward outbound messaging can further motivate active participation, reinforcing self-efficacy development.

Improving collective efficacy through group-oriented features. While active messaging predicted self-efficacy gains, it did not significantly influence community collective efficacy. Therefore, design strategies aiming to foster collective efficacy should emphasize group-oriented features, such as highlighting collective achievements, facilitating group discussions on privacy norms, or creating shared goals for privacy management. Visual indicators of collective progress can help form a sense of group accomplishment, distinct from individual confidence gains.

Raising awareness through visualized network. Interactive visualizations that map users' connections within the app can enhance awareness of communication patterns and potential biases in interaction networks. Visual elements that highlight frequently contacted peers, gaps in network diversity, or emergent clusters of similar privacy attitudes can serve as reflective tools, encouraging users to diversify their interactions and bridge network gaps.

Promoting diversity through nudges. The observed shift from initial heterophily to increased homophily indicates a tendency for users to gravitate towards like-minded peers over time. To counteract this, design elements that nudge users to engage with diverse network members can be implemented. These nudges can take the form of recommendations for users to engage with differing viewpoints or prompts to explore content from less frequently contacted peers. Such strategies can help address concerns about the reinforcement of pre-existing biases in online communities [22].

6.5 Limitations and Future Research

While the findings' internal validity is secured by the use of validated psychosocial scales and robust MRQAP network analysis with permutation testing, this study faced several limitations that warrant consideration when interpreting the findings, particularly regarding external validity (generalizability). Primarily, many participants were of a similar ethnic background, with strong ethnic homophily observed in group formation. While this provides a valuable case study of social dynamics within such a community, findings related to the pervasive role of ethnicity in initial group formation should be interpreted with caution and require further research in more diverse populations to validate their broader applicability. Similarly, the participant age distribution was notably unbalanced, with a strong concentration in young to middle adulthood (25-34 years), which may further limit the generalizability of our results to broader age demographics. Beyond the sample's composition, it is important to acknowledge that certain design affordances of the CO-oPS platform—such as the weekly prompts (e.g., "warn someone about unsafe permissions")—may have influenced interaction patterns. These prompts acted as a form of structured nudging, meaning the resulting behaviors were not purely organic. While this design choice ensured sufficient interaction data for analysis, it also likely guided users toward specific types of engagement, potentially accelerating the observed convergence of privacy perceptions. Additionally, while our study explored the influence of demographic homophily on interaction patterns, it did not directly assess the correlation between specific privacy settings (e.g., app permissions) and demographic factors such as age, ethnicity, or education. Furthermore, our data collection was impacted by the post-survey instrument, which did not include a power usage variable; this omission meant that the statistical model developed to predict the gains in CCE did not reach significance, suggesting that unmeasured factors influenced the outcome. Future work should aim to recruit more diverse participants and distinguish between naturally emergent social alignment and platform-induced interaction patterns. Additionally, incorporating a broader range of variables, potentially including power usage and other unexplored factors, such as power usage, will be important for developing more robust models to understand the multifaceted factors influencing community collective efficacy, as well as investigate how demographic characteristics directly influence granular privacy

settings and their evolution within collaborative privacy management contexts. Despite these limitations, key findings such as the positive influence of proactive messaging on individual self-efficacy gains are theoretically consistent with broader social learning theories and literature on knowledge sharing in online communities, suggesting their applicability extends beyond this specific study context.

7 Conclusion

Our study offered a comprehensive examination of how community formation and engagement influence individual and collective privacy and security efficacy. By integrating social network analysis with privacy perception constructs, we uncover the nuanced interplay between demographic similarity, attitudinal alignment, and user behavior in a community-centered privacy management context. Our findings demonstrate that while pre-existing social ties shape early patterns of engagement, it is proactive, outbound interaction—particularly through messaging—that predicts meaningful gains in individual self-efficacy. This insight, consistent with social learning theories, suggests a broad applicability for designing interventions that foster individual empowerment in digital contexts. Moreover, shifts from attitudinal heterophily to greater homogeneity over time suggest the emergence of shared privacy norms within digital communities. Beyond its empirical contributions, this work advances theoretical understandings of networked privacy by demonstrating how social configurations dynamically evolve in response to communal interaction. It highlights the importance of viewing privacy not solely as an individual concern, but as a socially embedded process shaped by relational structures and mutual accountability. These insights invite further interdisciplinary research that bridges CSCW, privacy theory, and behavioral science to deepen our understanding of how digital communities co-construct safety and trust in increasingly interconnected environments.

Acknowledgments

This research was supported by the U.S. National Science Foundation under grants CNS-1814068, CNS1814110, and CNS-2326901. 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] Mamtaj Akter, Leena Alghamdi, Dylan Gillespie, Nazmus Sakib Miazi, Jess Kropczynski, Heather Lipford, and Pamela J. Wisniewski. 2022. CO-OPS: A Mobile App for Community Oversight of Privacy and Security. In *Companion Publication of the 2022 Conference on Computer Supported Cooperative Work and Social Computing* (Virtual Event, Taiwan) *(CSCW'22 Companion)*. Association for Computing Machinery, New York, NY, USA, 179–183. doi:10.1145/3500868.3559706

[2] Mamtaj Akter, Leena Alghamdi, Jess Kropczynski, Heather Richter Lipford, and Pamela J. Wisniewski. 2023. It Takes a Village: A Case for Including Extended Family Members in the Joint Oversight of Family-Based Privacy and Security for Mobile Smartphones. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI EA '23)*. Association for Computing Machinery, New York, NY, USA, Article 194, 7 pages. doi:10.1145/3544549.3585904

[3] Mamtaj Akter, Amy J. Godfrey, Jess Kropczynski, Heather R. Lipford, and Pamela J. Wisniewski. 2022. From Parental Control to Joint Family Oversight: Can Parents and Teens Manage Mobile Online Safety and Privacy as Equals? *Proc. ACM Hum.-Comput. Interact.* 6, CSCW1, Article 57 (apr 2022), 28 pages. doi:10.1145/3512904

[4] Adriana Alvarado Garcia, Tianling Yang, and Milagros Miceli. 2025. What Knowledge Do We Produce from Social Media Data and How? *Proc. ACM Hum.-Comput. Interact.* 9, 1, Article GROUP37 (Jan. 2025), 45 pages. doi:10.1145/3701216

[5] Panagiotis Andriotis, Shancang Li, Theodoros Spyridopoulos, and Gianluca Stringhini. 2017. A Comparative Study of Android Users' Privacy Preferences Under the Runtime Permission Model. In *Human Aspects of Information Security, Privacy and Trust: 5th International Conference, HAS 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings* (Vancouver, BC, Canada). Springer-Verlag, Berlin, Heidelberg, 604–622. doi:10.1007/978-3-319-58460-7_42

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

[7] Albert Bandura. 1997. *Self-efficacy: The exercise of control.* W. H. Freeman.

[8] Lior Bar-Achel, Sarit Kraus, Omer Lev, and Shay Mozes. 2018. Helping others helps yourself: The effect of providing help on helper's task performance. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. ACM, 1–12.

[9] Guido Barbian. 2011. Trust Centrality in Online Social Networks. In *2011 European Intelligence and Security Informatics Conference*. 372–377. doi:10.1109/EISIC.2011.17

[10] Francesco Bonchi, Carlos Castillo, Aristides Gionis, and Alejandro Jaimes. 2011. Social Network Analysis and Mining for Business Applications. *ACM Trans. Intell. Syst. Technol.* 2, 3, Article 22 (May 2011), 37 pages. doi:10.1145/1961189.1961194

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

[12] Stephen Borgatti and Daniel Halgin. 2014. Analyzing Affiliation Networks. In *The SAGE Handbook of Social Network Analysis*, John Scott and Peter J. Carrington (Eds.). SAGE Publications Ltd, 417–433. doi:10.4135/9781446294413.n28

[13] Stephen P Borgatti, Filip Agneessens, Jeffrey C Johnson, and Martin G Everett. 2024. *Analyzing social networks.* SAGE publications Ltd.

[14] Stephen P Borgatti, Ajay Mehra, Daniel J Brass, and Giuseppe Labianca. 2009. Network analysis in the social sciences. *Science* 323, 5916 (2009), 892–895.

[15] Paolo Calciati, Konstantin Kuznetsov, Alessandra Gorla, and Andreas Zeller. 2020. Automatically Granted Permissions in Android Apps: An Empirical Study on Their Prevalence and on the Potential Threats for Privacy. In *Proceedings of the 17th International Conference on Mining Software Repositories* (Seoul, Republic of Korea) *(MSR '20)*. Association for Computing Machinery, New York, NY, USA, 114–124. doi:10.1145/3379597.3387469

[16] J.M. Carroll and D.D. 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.* Institute of Electrical and Electronics Engineers, Big Islane, HI, USA, 10 pp.–. doi:10.1109/HICSS.2003.1174585

[17] 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* (Portland, Oregon, USA) *(CHI '05)*. Association for Computing Machinery, New York, NY, USA, 1–10. doi:10.1145/1054972.1054974

[18] Salvatore A. Catanese, Pasquale De Meo, Emilio Ferrara, Giacomo Fiumara, and Alessandro Provetti. 2011. Crawling Facebook for social network analysis purposes. In *Proceedings of the International Conference on Web Intelligence, Mining and Semantics* (Sogndal, Norway) *(WIMS '11)*. Association for Computing Machinery, New York, NY, USA, Article 52, 8 pages. doi:10.1145/1988688.1988749

[19] Francesca Cerruto, Stefano Cirillo, Domenico Desiato, Simone Michele Gambardella, and Giuseppe Polese. 2022. Social network data analysis to highlight privacy threats in sharing data. *Journal of Big Data* 9, 1 (2022), 19.

[20] 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, Article 146 (nov 2019), 31 pages. doi:10.1145/3359248

[21] Giulio Cimini, Tiziano Squartini, Fabio Saracco, Diego Garlaschelli, Andrea Gabrielli, and Guido Caldarelli. 2019. The statistical physics of real-world networks. *Nature Reviews Physics* 1, 1 (2019), 58–71.

[22] Matteo Cinelli, Gianmarco De Francisci Morales, Alessandro Galeazzi, Walter Quattrociocchi, and Michele Starnini. 2021. The echo chamber effect on social media. *Proceedings of the national academy of sciences* 118, 9 (2021), e2023301118.

[23] Julián D Cortés and María Catalina Ramírez Cajiao. 2024. The policy is dead, long live the policy—Revealing science, technology, and innovation policy priorities and government transitions via network analysis. *Quantitative Science Studies* 5, 2 (2024), 317–331.

[24] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A. Dabbish, and Jason I. Hong. 2014. The Effect of Social Influence on Security Sensitivity. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security* (Menlo Park, CA) *(SOUPS '14)*. USENIX Association, USA, 143–157.

[25] D. Dekker, D. Krackhardt, and T.A.B. Snijders. 2007. Sensitivity of MRQAP tests to colliniarity and autocorrelation conditions. *Psychometrika* 72, 4 (2007), 563–581.

[26] Judith S. Donath. 1999. Identity and deception in the virtual community. In *Communities in cyberspace*. Routledge, 29–59.

[27] Islam H. El-adaway, Ibrahim S. Abotaleb, and Eric Vechan. 2017. Social Network Analysis Approach for Improved Transportation Planning. *Journal of Infrastructure Systems* 23, 2 (2017), 05016004. doi:10.1061/(ASCE)IS.1943-555X.0000331

[28] Federal Trade Commission. [n. d.]. Children's Online Privacy Protection Act. Web page. https://www.ftc.gov/legal-library/browse/statutes/childrens-online-privacy-protection-act

[29] Susan R Fussell, Robert E Kraut, and Jane Siegel. 2000. Coordination of communication: Effects of shared visual context on collaborative work. In *Proceedings of the 2000 ACM conference on Computer supported cooperative work*. 21–30.

[30] Reza Ghaiumy Anaraky, Kaileigh Angela Byrne, Pamela J. Wisniewski, Xinru Page, and Bart Knijnenburg. 2021. To Disclose or Not to Disclose: Examining the Privacy Decision-Making Processes of Older vs. Younger Adults. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 686, 14 pages. doi:10.1145/3411764.3445204

[31] Daniel Z Grunspan, Benjamin L Wiggins, and Steven M Goodreau. 2014. Understanding classrooms through social network analysis: A primer for social network analysis in education research. *CBE—Life Sciences Education* 13, 2 (2014), 167–178. doi:10.1187/cbe.13-08-0162

[32] Oskar J Gstrein and Anne Beaulieu. 2022. How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy & Technology* 35, 1 (Jan. 2022), 3. doi:10.1007/s13347-022-00497-4

[33] Penelope Hawe, Cynthia Webster, and Alan Shiell. 2004. A glossary of terms for navigating the field of social network analysis. *Journal of Epidemiology & Community Health* 58, 12 (2004), 971–975. arXiv:https://jech.bmj.com/content/58/12/971.full.pdf doi:10.1136/jech.2003.014530

[34] Caroline Haythornthwaite. 2002. Strong, weak, and latent ties and the impact of new media. *The Information Society* 18, 5 (2002), 385–401.

[35] Corey Brian Jackson and Yang Wang. 2018. Addressing The Privacy Paradox through Personalized Privacy Notifications. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 2 (July 2018), 1–25. doi:10.1145/3214271

[36] Terrence D. Jorgensen, Katelyn J. Forney, Judith A. Hall, and Scott Giles. 2018. Using Modern Methods for Missing Data Analysis with the Social Relations Model: A Bridge to Social Network Analysis. *Social Networks* 54 (2018), 26–40. doi:10.1016/j.socnet.2017.11.002

[37] David Krackhardt and Robert N. Stern. 1988. Informal networks and organizational crises: an experimental simulation. *Social Psychology Quarterly* 51, 2 (1988), 123–140.

[38] Jess Kropczynski, Reza Ghaiumy Anaraky, Mamtaj Akter, Amy J. Godfrey, Heather Lipford, and Pamela J. Wisniewski. 2021. Examining Collaborative Support for Privacy and Security in the Broader Context of Tech Caregiving. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 396 (oct 2021), 23 pages. doi:10.1145/3479540

[39] Chih-Hao Ku and Gondy Leroy. 2014. A decision support system: Automated crime report analysis and classification for e-government. *Government Information Quarterly* 31, 4 (2014), 534–544. doi:10.1016/j.giq.2014.08.003

[40] Barbara S. Lawrence and Neha Parikh Shah. 2020. Homophily: Measures and Meaning. *Academy of Management Annals* 14, 2 (2020), 513–597. Barbara S. Lawrence: Anderson Graduate School of Management, University of California Los Angeles; Neha Parikh Shah: Rutgers Business School-Newark & New Brunswick, Rutgers University.

[41] Bin Liu, Jialiu Lin, and Norman Sadeh. 2014. Reconciling mobile app privacy and usability on smartphones: could user privacy profiles help?. In *Proceedings of the 23rd International Conference on World Wide Web* (Seoul, Korea) *(WWW '14)*. Association for Computing Machinery, New York, NY, USA, 201–212. doi:10.1145/2566486.2568035

[42] Raudelio Machin Suarez and Diana Viscay Mantilla. 2021. *From Virtual Communities to Research on Virtuality: Emerging Concepts and Research Challenges—Ethnographic Research in the Digital Age.* Springer International Publishing, Cham, 223–255. doi:10.1007/978-3-030-87406-3_10

[43] Miller McPherson, Lynn Smith-Lovin, and James M Cook. 2001. Birds of a Feather: Homophily in Social Networks. *Annual Review of Sociology* 27, Volume 27, 2001 (2001), 415–444. doi:10.1146/annurev.soc.27.1.415

[44] Tamir Mendel and Eran Toch. 2017. Susceptibility to social influence of privacy behaviors: Peer versus authoritative sources. In *Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing*. 581–593. https://dl.acm.org/doi/10.1145/2998181.2998323

[45] Tamir Mendel and Eran Toch. 2023. Social Support for Mobile Security: Comparing Close Connections and Community Volunteers in a Field Experiment. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, Article 590.

[46] Michael Mitchell, Ratnesh Patidar, Manik Saini, Parteek Singh, An-I Wang, and Peter Reiher. 2015. Mobile usage patterns and privacy implications. In *2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*. 457–462. doi:10.1109/percomw.2015.7134081

[47] Helen Nissenbaum. 2009. Privacy in context: Technology, policy, and the integrity of social life. In *Privacy in context*. Stanford University Press.

[48] E. Pan, J. Ren, M. Lindorfer, C. Wilson, and D. Choffnes. 2018. Panoptispy: characterizing audio and video exfiltration from android applications. *Proceedings on Privacy Enhancing Technologies* 2018 (2018), 33–50. Issue 4. doi:10.1515/popets-2018-0030

[49] Emilee Rader and Rick Wash. 2015. Identifying patterns in informal sources of security information. *Journal of Cybersecurity* 1, 1 (Sept. 2015), 121–144. doi:10.1093/cybsec/tyv008 Publisher: Oxford Academic.

[50] Erhard Rahm, Hong Hai Do, et al. 2000. Data cleaning: Problems and current approaches. *IEEE Data Eng. Bull.* 23, 4 (2000), 3–13.

[51] Bahman Rashidi, Carol Fung, Anh Nguyen, Tam Vu, and Elisa Bertino. 2018. Android User Privacy Preserving Through Crowdsourcing. In *IEEE Transactions on Information Forensics and Security*, Vol. 13. IEEE, 773–787.
[52] Joel Reardon, Álvaro Feal, Primal Wijesekera, Amit Elazari Bar On, Narseo Vallina-Rodriguez, and Serge Egelman. 2019. 50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System. In *WINTER 2019, VOL. 44, NO. 4* (2019). USENIX, Boston, MA, United States, 603–620. https://www.usenix.org/conference/usenixsecurity19/presentation/reardon
[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] Elizabeth M. Reid. 1996. Cultural formations in text-based virtual realities. *Cyberspace: First steps* (1996), 143–167.
[55] Androniki Sapountzi and Kostas E. Psannis. 2018. Social networking data analysis tools & challenges. *Future Generation Computer Systems* 86 (2018), 893–913. doi:10.1016/j.future.2016.10.019
[56] John Scott. 1988. Trend report social network analysis. *Sociology* (1988), 109–127.
[57] Y. Shvartzshnaider, S. Tong, T. Wies, P. Kift, H. Nissenbaum, L. Subramanian, and P. Mittal. 2016. Learning Privacy Expectations by Crowdsourcing Contextual Informational Norms. *Proceedings of the AAAI Conference on Human Computation and Crowdsourcing* 4 (2016), 209–218. doi:10.1609/hcomp.v4i1.13271
[58] Shashank Sheshar Singh, Samya Muhuri, Sumit Kumar, and Jayendra Barua. 2025. From Nodes to Knowledge: Exploring Social Network Analysis in Education. *ACM Trans. Web* 19, 1, Article 7 (Jan. 2025), 36 pages. doi:10.1145/3707463
[59] Shashank Sheshar Singh, Samya Muhuri, Shivansh Mishra, Divya Srivastava, Harish Kumar Shakya, and Neeraj Kumar. 2024. Social Network Analysis: A Survey on Process, Tools, and Application. *ACM Comput. Surv.* 56, 8, Article 192 (April 2024), 39 pages. doi:10.1145/3648470
[60] D. Smullen, Y. Feng, S. Zhang, and N. Sadeh. 2020. The best of both worlds: mitigating trade-offs between accuracy and user burden in capturing mobile app privacy preferences. *Proceedings on Privacy Enhancing Technologies* 2020 (2020), 195–215. Issue 1. doi:10.2478/popets-2020-0011
[61] 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.
[62] Gioacchino Tangari, Muhammad Ikram, Kiran Ijaz, Mohamed Ali Kaafar, and Shlomo Berkovsky. 2021. Mobile health and privacy: cross sectional study. *BMJ* 373 (2021). arXiv:https://www.bmj.com/content/373/bmj.n1248.full.pdf doi:10.1136/bmj.n1248
[63] Emily A. Vogels and Monica Anderson. 2019. Americans and Digital Knowledge. *Pew Research* (Oct. 2019). https://www.pewresearch.org/internet/2019/10/09/americans-and-digital-knowledge/
[64] Zhiyuan Wan, Lingfeng Bao, Debin Gao, Eran Toch, Xin Xia, Tamir Mendel, and David Lo. 2020. AppMoD: Helping Older Adults Manage Mobile Security with Online Social Help. In *Proceedings of the ACM Interact. Mob. Wearable Ubiquitous Technol.*, Vol. 3. ACM, Article 154.
[65] Molly McLure Wasko and Samer Faraj. 2004. Knowing in networks: Individual and collective expertise in an electronic network of practice. *Organization science* 15, 6 (2004), 671–688.
[66] Paul Widdop. 2025. Sport social network analysis. In *Handbook of Culture and Social Networks*. Edward Elgar Publishing, 121–138.
[67] Debra L Worthington and Margaret Fitch-Hauser. 2019. Communication privacy management and mobile phone use. In *Cloud Security: Concepts, Methodologies, Tools, and Applications*. IGI Global, 1829–1843. doi:10.4018/978-1-4666-8239-9.ch075
[68] V. Wottrich, E. Reijmersdal, and E. Smit. 2018. App users unwittingly in the spotlight: a model of privacy protection in mobile apps. *Journal of Consumer Affairs* 53 (2018), 1056–1083. Issue 3. doi:10.1111/joca.12218
[69] Leming Zhou, Bambang Parmanto, Zakiy Alfikri, and Jie Bao. 2018. A Mobile App for Assisting Users to Make Informed Selections in Security Settings for Protecting Personal Health Data: Development and Feasibility Study. *JMIR Mhealth Uhealth* 6, 12 (11 Dec 2018), e11210. doi:10.2196/11210
[70] Yingyi Zhou, Claudia Tagliaro, and Ying Hua. 2021. Networked "bubbles": study workgroups' spatial adjacency preference using social network analysis methods. *Journal of Corporate Real Estate* 23, 2 (2021), 87–105. doi:10.1108/JCRE-06-2020-0024
[71] Hengshu Zhu, Hui Xiong, Yong Ge, and Enhong Chen. 2014. Mobile App Recommendations with Security and Privacy Awareness. In *Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (New York, New York, USA) *(KDD '14)*. Association for Computing Machinery, New York, NY, USA, 951–960. doi:10.1145/2623330.2623705

Received May 2025; revised November 2025; accepted December 2025