# “We Hold Each Other Accountable”: Unpacking How Social Groups Approach Cybersecurity and Privacy Together

**Hue Watson, Eyitemi Moju-Igbene, Akanksha Kumari, Sauvik Das**
Georgia Institute of Technology
Atlanta, GA, USA
huewatson@protonmail.com, {moju, akanksha.kumari, sauvik}@gatech.edu

## ABSTRACT

Digital resources are often collectively owned and shared by small social groups (e.g., friends sharing Netflix accounts, roommates sharing game consoles, families sharing WhatsApp groups). Yet, little is known about (i) how these groups jointly navigate cybersecurity and privacy (S&P) decisions for shared resources, (ii) how shared experiences influence individual S&P attitudes and behaviors, and (iii) how well existing S&P controls map onto group needs. We conducted group interviews and a supplemental diary study with nine social groups (n=34) of varying relationship types. We identified why, how and what resources groups shared, their jointly construed threat models, and how these factors influenced group strategies for securing shared resources. We also identified missed opportunities for cooperation and stewardship among group members that could have led to improved S&P behaviors, and found that existing S&P controls often fail to meet the needs of these small social groups.

### Author Keywords

Privacy; Security; Interviews; Qualitative Methods; Social Cybersecurity; Groups

### CCS Concepts

**•Security and privacy → Social aspects of security and privacy; •Human-centered computing → Human computer interaction (HCI);**

## INTRODUCTION

We live in an era of social computing. Today, many valuable digital resources (e.g., documents, accounts, devices) are collectively owned and shared by a range of small, social groups (e.g., families, friends, partners, colleagues) [4, 13, 19, 24, 28]. This gradual transition from personal to social computing complicates the design of end-user controls for maintaining the cybersecurity and digital privacy of digital resources (commonly abbreviated as S&P) [10, 24].

**Figure 1. We investigated how small, social groups jointly construe S&P policies to protect their shared digital resources (e.g., game consoles, streaming services, IoT devices). Existing S&P controls poorly mapped onto socially construed strategies for protecting shared resources.**

Indeed, with shared streaming accounts for entertainment, document storage and collaboration services, communication platforms, edge computing devices, and IoT appliances, notions of ownership and access control for digital resources can vary across a spectrum from *individual ownership and use* to an interwoven, *networked* model in which resources are *collectively owned, shared and used* [4, 19, 24, 27].

Yet, in designing the controls to help people maintain the security and privacy of these protected, shared resources, designers often make simplifying assumptions that can be socially inappropriate [7, 10]: e.g., that one person owns and controls access to a digital resource; that they should be the person who initially creates, purchases or initializes the resource; and, that everyone who accesses a digital resource has a distinct account against which access policies can be enforced. These assumptions simplify the creation of S&P controls, but do they hold when resources are collectively owned and shared?

A Netflix account may be shared by five close friends who each contribute to a monthly subscription [17], but what if one of these friends wants to keep their watching history private? A smart thermostat may have one owner, or may be owned

*CHI '20, April 25–30, 2020, Honolulu, HI, USA.*
Copyright is held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-6708-0/20/04 ...$15.00.
http://dx.doi.org/10.1145/3313831.3376605

and used by a whole family, but what if family dynamics necessitate prioritizing access to parents over children? [19] Parents may want to share photos of their teenage children on Facebook, but what happens when the teenagers in those pictures do not want those pictures shared? [23] More generally, to paraphrase Ackerman [1], it remains unclear how these simplified technical controls for maintaining the S&P of digital resources align with the social requirements of the small groups who collectively own, create and share these resources. Understanding this connection is essential if we are to design S&P controls that better cater to these groups.

Recent prior work in usable privacy and security has found both observational and experimental evidence that social influences affect individuals' attitudes and behaviors towards S&P [7, 8, 9, 30, 31]. Indeed, prior work in usable privacy and security suggests that end-user attitudes and behaviors towards S&P can be formed through dialectic processes [27, 30], e.g., through exposure to vulnerabilities, others' experiences and behaviors, and a subsequent social sense-making process [7, 11, 16]. As such, as people increasingly navigate decisions to maintain the S&P of jointly owned resources in small, social groups, it seems plausible that these group social interactions should then influence individual group members' attitudes towards S&P more generally. Accordingly, in this work, we pose the following broad research questions:

- **RQ1:** *How do small, social groups (e.g., close friends, coworkers, families) jointly navigate decisions to secure protected, shared resources?*
- **RQ2:** *How do the shared experiences and interactions of small, social groups influence each member's attitudes and behaviors towards S&P, in general?*

To answer these questions, we conducted in-person, semi-structured *group interviews* with nine distinct social groups of 3 - 5 participants each ($n = 34$). We supplemented these interviews with a 4-week diary study where each participant was prompted to regularly document conversations, thoughts and interactions they had about S&P, generally, as well as how and why they shared those experiences with their groups, if at all. We investigated the protected, shared resources they shared, the collectively emergent threat models that these groups were concerned with, and the in-group social dynamics and how all of these factors interacted in decision-making processes regarding S&P in the group setting.

We defined **protected, shared resources**[1] as *any tool, service or space that was jointly owned and/or accessed by group members but that were generally not meant to be seen or used by those outside of the group*.

We found that groups varied widely in the types of resources they shared and tried to protect, ranging from digital media accounts like Netflix to edge computing devices like home gaming consoles. Groups also varied in the threat models they found pertinent to protect against: some were focused on insider threats, others on outsider threats, and still others on a hybrid model of outsider threats resulting from insider negligence. Strategies for securing resources against these threats were primarily *socially construed*, implicit, and enforced with little support from existing technical controls (see Figure 1). Indeed, individual group members were expected to uphold implicitly defined, often unspoken access and security norms to group resources. However, these strategies were not enforceable and led to inequity, inefficiency and resentment: participants expressed frustration that even if they invested individual effort into securing resources, that effort could be undermined by others' weak S&P practices.

We conclude by identifying a number of social-technical gaps between what is possible with existing S&P controls for digital resources and what social groups actually want and need in those controls. Addressing these gaps should help improve the S&P practices of the increasing numbers of small, social groups who collectively own and share digital resources.

## RELATED WORK

### Tensions Between Social Norms and Interface Affordance

In describing the core intellectual challenge of Computer-Supported Cooperative Work (CSCW), Ackerman describes a social-technical gap between what current technologies are capable of doing and what they *need to be able to do* in order to adequately support the social contexts in which they are embedded [1]. In the context of S&P, Dourish and Anderson made the case that S&P are social phenomena and should be approached as such [12]. From sharing passwords with partners and coworkers [20] to sharing edge devices in households [24], everyday people share "personal" digital resources with others. While prior work has not specifically examined how well S&P controls align with the social needs of end-users, a wealth of prior work has alluded to the idea that existing S&P controls are often too rigid to adequately capture and support the social needs of small groups of individuals who collectively own and share digital resources [7, 23, 26]. Accordingly, these groups often find workarounds, by, for example, sharing passwords with friends and loved ones [10, 35].

Collaboration between social and technical researchers can help bridge this gap [29]. Our work aims to explore how groups of socially connected individuals navigate decisions to secure shared resources and how existing S&P controls map onto their preferences and needs. With the ultimate goal of developing technical solutions to combat problems faced, our findings should inform the design of S&P controls that seamlessly integrate into the social contexts of small groups, helping to alleviate the social-technical gap between S&P controls that exist today and the S&P controls that groups of socially connected individuals need.

### The Motivation, Needs and Complications Behind Sharing

Several studies have explored the motivations underlying the sharing behaviors of socially-connected groups [4, 18, 24, 28]. Matthew *et al.*'s research on households established a taxonomy of sharing types ranging from borrowing to accidental. Also, across their sharing taxonomies, the motivations for sharing were highly influenced by trust in the sharee or convenience [24]. Jacobs *et al.*'s study of co-habitating couples

[1] We may refer to these protected, shared resources simply as *resources*

identified how sharing occurs and classified shared information into three categories; public content, tailored content and personal conversation [18]. Park *et al.* conducted a survey with 195 participants in relationships and found that couples' level of sharing evolves as the relationship progresses — the initial phases, during the relationship and after a breakup [28]. Marwick and Boyd [23] showed how sharing social information online raised *networked* tensions between the person sharing the content and the subjects of the content. Our study adds another dimension on these areas by investigating groups' security practices and behaviors for the resources and data they share with and about their groups.

Other studies offer prescriptive insights into how to design S&P controls for specific group use-cases. Brush & Inkpen's study of fifteen families suggest that household technology devices which are usually designed with either the appliance or profile sharing model in mind might be more beneficial if designed with a mixed model to better cater to household sharing behaviors [4]. Egelman's testing of mixed model family accounts showed that families preferred them over what they were using currently (either one shared account or several individual profiles) [13]. Initial feedback on a prototype for group recommendations on Netflix showed promise in its appeal to households with multiple viewers [2]. We build on this by taking a more general approach: rather than focus on a single group structure, we explore a range of small, social groups and take an open-ended approach towards exploring the resources they share, the threat models they seek to protect against, and the strategies they employ to protect those shared resources against those threat models.

### Social Influences on Cybersecurity and Privacy

Recently, there has been increasing interest in studying how social influences impact end-user S&P attitudes and behaviors. Das *et al.* showed that social triggers can strongly motivate people to adopt better security practices or at least lead to an increased awareness for security [6, 7, 8]. Gaw *et al.* [16] found that the context of S&P control usage affected end-user perceptions of the people who used those controls. If people encrypted communications that were deemed not to be sensitive, they could be perceived as paranoid. Das *et al.* [9] later argue that this paranoia-effect can stilt the adoption of S&P controls because people do not want to be perceived as paranoid. Rader *et al.* show how informal stories and narratives, passed on colloquially from one person to another, can also strongly influence S&P attitudes and behaviors. By conducting studies with participants comprising of five different sections of undergraduate telecommunications classes [30]. Specifically, autobiographical narratives seemed to have the greatest impact on people for changing their behavior. This shows that people value experiences of others and it could be a trigger to make a change in their security practices. Our study contributes to this literature by exploring how the shared S&P experiences of small, social groups — or the lack thereof — influences both group and individual S&P decision-making.

### Group Dynamics

Social groups come in varied forms. An early top-level categorization of these groups splits social groups into two broad kinds: *common bond* groups, who are bound by intimacy (e.g., families, close friends), and *common identity* groups, who are bound by purpose or interest (e.g., project groups, people who like tennis) [33]. Studies have shown that these dynamics — common-bond vs. common-identity — lead to different kinds of attachments to shared platforms among those groups [15, 32]. These differences, in turn, could influence the strategies different groups might employ to secure shared resources (e.g., families may have malleable access control boundaries, where work colleagues may not). Given the behavioral and interpersonal differences of common-bond versus common-identity groups and its potential bearing on shared S&P, we recruited social groups of both kinds.

## METHODOLOGY

### Recruitment

We recruited groups for in-person interviews using convenience sampling through a variety of online (Facebook, Twitter, Nextdoor, Craigslist) and offline (canvasing and posting fliers) methods. Groups were all local to Atlanta, GA where our institution, Georgia Institute of Technology, is located. Potential participant groups needed to have known each other for at least 6 months and have actively shared a digital resource. Requirements for eligibility were included on recruitment documents. We also verified eligibility through a screening questionnaire, included in the supplementary materials. Our study ran for a seven-month period between May and December of 2018, and participants could receive a maximum of $47 in incentives.

### Participants

We recruited thirty-four participants split across nine social groups[2]. Participants filled out a demographic questionnaire and Egelman and Peer's security behavioral intention scale [14], which broadly measures the extent of an individual's intention to follow expert-recommended cybersecurity advice.

For the subset of participants whose demographics we are able to share[3], participants were aged 18 to 30 years old, comprised of more males (52%) than females (29%)[3], and had varied levels of education (High School - 44%, Bachelors - 17%, Masters - 15%, Post Graduate - 6%))[3]. Most of our participants identified as Asian or White (Asian - 35%, White - 32% , Hispanic - 6%, Black - 3%)[3]. Groups were comprised of 3-5 people who had known each other for at least six months, and their composition is shown in Table 1.

### Procedure

We conducted an IRB-approved study in order to answer our research question — namely, to gain insight into how groups of socially connected individuals jointly navigate S&P decisions over collectively owned and shared resources, and how group members influence one another's attitudes and behaviors towards S&P. Broadly, our study consisted of two parts: (i) a sixty-minute semi-structured group interview to understand

[2] Detailed participant demographics available in Table S1 in the supplementary materials

[3] Owing to a minor deviance in our demographic questionnaire and what was approved in our IRB application.

| Group | Relationship | N |
|---|---|---|
| A | Family | 4 |
| B | Family | 4 |
| C | Classmates | 3 |
| D | Close Friends | 5 |
| E | Close Friends | 3 |
| F | Close Friends, Roommates | 5 |
| G | Coworkers | 3 |
| H | Roommates | 3 |
| I | Close Friends, Roommates | 4 |

**Table 1. Group Dynamics (P = 34). Groups are categorized based on their relationship types. Our study interviewed nine groups ranging from family, classmates, close friends, roommates, and coworkers. Each group consisted of three to five members who had known each other for a least six months.**

group S&P behaviors and practices; and, (ii) a supplementary 4-week diary study with phone interviews to gather in situ data of S&P behaviors over a period of time.

### Group Interviews

We started with a semi-structured group interview to get a broad understanding of the structural, social and contextual factors that defined and affected each group, their individual and group security needs and threat models, and their interactions and missed interactions around S&P. Interviews were in person and were audio and video recorded to facilitate data analysis. The complete set of questions we asked each group during the semi-structured interview are provided in the supplementary materials.

### Supplemental Diary Study

Following the group interview, participants were enrolled in a 4-week Ecological Momentary Assessment(EMA) diary study [34] to gather data of their S&P-related behaviors and correspondences closer, in time, to when they occurred. For this phase of the study, participants were asked, three times per week, to fill out a brief questionnaire on their recent S&P-related conversations and behaviors using the PACO smartphone app[4]. The diary study provided further qualitative feedback to support interview findings. From the thirty-four participants, we had a total of 395 diary study entries. We list the complete set of questions that were asked in our diary study in the supplementary materials.

### Phone Interviews

Throughout the duration of the diary study, we conducted short (15-minute) phone interviews to follow up on participants' diary study responses. As this interview was based off the responses from the diary study, exact questions varied, but the broad format of the questions we asked are listed in the supplementary materials.

## Data Analysis

We used a mixed inductive and deductive approach for our thematic analysis [3] in analyzing and coding the group interviews, the open-ended diary study responses, and any embellishments participants provided to these responses in the complementary phone interview. This analysis was conducted by three researchers, two of whom collaboratively engaged in reviewing transcripts to develop a single codebook, generating fifty-nine codes. The same two researchers used this codebook to analyze each transcript to find emergent patterns and themes across the data corpus, such as 'accountability for security information/resources' or 'prompting security behaviors.' A third researcher then met with the other two to discuss themes until an agreement was reached.

For the closed-ended diary study responses, we primarily calculated descriptive statistics: for example, the percentage of our participants who reported having an S&P related conversation during the study period, or the number of behavior changes that resulted from a group interaction.

## RESULTS

To answer our RQs, we start by typifying the resources our groups shared and why they were shared, what threat models they believed they were facing, and how these factors interacted with strategies for securing their resources. We discuss how individual security practices implicitly formed the basis of each group's strategy for securing their resources, often resulting in a situation where the security of a resource reduced down to the practices of the group member who had the weakest security behaviors. We then discuss how shared experiences and interactions between group members sometimes influenced attitudes towards S&P more generally, but also identified a number of missed opportunities for sharing S&P behaviors and information that arose from a marked *absence* of S&P related interactions among group members.

## Shared Group Resources & Behavioral Triggers for S&P

Before we could assess the strategies groups employed to secure their protected, shared resources (RQ1) or how group S&P interactions influenced individual group members (RQ2), we first needed to understand the dynamics of the groups, themselves, and the resources they shared. Accordingly, we started by asking groups about their protected, shared resources. These resources spanned five distinct categories: *digital media accounts*, such as shared Netflix or Hulu accounts; *physical items* such as cars, fridges and televisions, which are increasingly being embedded with computation and are likely to have increasing S&P relevance in the near future; *edge computing devices*, such as iPads, WiFi routers and game consoles; *group chats and messengers*, such as WhatsApp and GroupMe; and, *social media* correspondences on services such as Venmo, Facebook groups, and Snapchat. For a full list of the resources that groups shared, see Table 2.

### Why do Groups Share Resources?

Knowing what groups shared, we next explored why those resources were shared. Drawing inspiration partially from Matthews *et al.*'s taxonomy of sharing types [24], we discovered that our participant groups shared resources for three reasons: (i) *to maintain a digital connection*, (ii) *for mutual use*, and (iii) *for borrowing*.

### *Maintaining a Digital Connection*

Groups shared communication channels and digital spaces (i.e., Group Messaging, Social Media in Table 2) as a way

[4] https://www.pacoapp.com/

| Resource Categories | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Digital Media Accounts | | Physical Items | | Edge Computing Devices | | Group Messaging | | Social Media | |
| **Resource** | **Group** | **Resource** | **Group** | **Resource** | **Groups** | **Resource** | **Groups** | **Resource** | **Group** |
| Netflix | A,B,H | Cars | A,B,F | iPad | A | GroupMe | B,I | Facebook | C |
| Google Play | A,F | Fridge | F | WiFi | F,H | WhatsApp | C | Find my friends | D |
| Hulu | B | Furniture | F,I | PlayStation | I | iMessage | D,E | Snapchat | E,F |
| Spotify | B | T.V. | H | Nintendo Switch | I | Google Voice | E | Instagram | E |
| Amazon | H,I | | | Chegg | I | Not specified | H | Venmo | F |
| HBO | H | | | | | Text messaging | E, G | | |
| | | | | | | Facebook Messenger | I | | |

**Table 2. Shared Resources Categorized by Type and Group. Resources that were shared have been organized into fix distinct types: Digital Media Accounts, Physical Items, Edge Computing Devices, Group Messaging, and Social Media. These shared resources helped groups maintain a digital connection, and facilitated mutual use as well as borrowing among members.**

to maintain a persistent digital connection with one another. They viewed these shared resources as tools to help keep in touch and stay safe. Unsurprisingly, almost all groups used some sort of group messaging application for general communication, coordination, and planning. Close groups like group D also considered location sharing important. For example, by providing real-time location updates for each group member, the iPhone's Find My Friend service [5] helped provide individuals peace-of-mind that their group members were safe. As group D stated:

> D1: I started that [iPhone's Find My Friend], ...because all the time there's somebody who's asking where are you, where are you? So I said oh, everyone just share their location then now we can see.
> D5: With like security it helps, whenever someone's out and we don't know where they are.
> D1: So if they say, 'oh I'm going out with this person,' we can see their location.

*Mutual Use*
Groups in our study also shared digital resources for *mutual use*. Here we define mutual use using Matthew *et al.*'s taxonomy of sharing types: "2+ people regularly use device/account as one of their primary of that type"[24]. Cost savings, in particular, was a key motivator for sharing Digital Media Accounts for mutual use. For example, when discussing the value of group H's digital media resources (e.g Netflix), H3 said *"[It] is a way to cut the cost."*

Some Physical Items and Edge Computing Devices were also shared for entertainment purposes. Using a shared device like a console, TV, or computer was a common practice that groups, like group D and I, employed to access streaming media services. In these cases, account passwords were shared and group members were able to access media on their own time, or group members used these resources to spend in-person time with each other. For example, group H used their shared Netflix and HBO accounts on their shared TV to bond over dinner:

> H1: We have a shared TV [that we use for Netflix and HBO] so we hang out in those shared spaces a lot. Bonding time.
> H2: We generally like dinner together. Which we have on most days.

*Borrowing*
Some groups, particularly A and B, mentioned borrowing each other's Physical Items and Edge Computing Devices. Again, our findings support Matthew *et al.*'s definition of borrowing in their taxonomy of sharing types: "temporary lending that benefits the sharee" [24]. The ability to use each other's devices when needed is a benefit they took advantage of frequently. When discussing the reason for sharing personal smartphones, A1 said, *"If [a group member] wanted to go on my phone or if his phone is dead, or if there are certain things he wants to do on my phone since I have Apple, then he can come on my phone and do it, and same thing with his, since he has Android, and I can go on his phone and um, and do the Google app or Netflix."*

### RQ1: How Do Groups Secure Their Shared Resources?

With an understanding of what kinds of resources groups are sharing and why, we next discuss the strategies our participant groups employed to secure these resources (RQ1). In analyzing these strategies, however, we first considered context — namely, what jointly construed threat models were groups attempting to protect against and what prompted their consideration of specific S&P strategies at all. Following this

[5] https://support.apple.com/en-us/HT201493

exploration of context, we codified specific strategies that our participant groups employed.

### Group Threat Models

Any discussion of security strategies must begin with an understanding of what those strategies are meant to protect against. The background literature in usable privacy and security has codified a set of "folk" threat models that individual end-users aim to protect against (e.g., [37]), but less is known about the threat models that groups of socially connected individuals might *jointly construe*. We bridge this gap in the literature here. In brief, our participant groups protected against one of three threat models: threats from other people in the group, threats from strangers and outsiders, and threats from outsiders that might be facilitated by fellow group members.

*Insider threats (Groups E & G)* are threats from within the group. Group G stated that they trusted each other to the point that they became less secure and took their security for granted when around each other. They worried that this implicit trust could, in turn, expose them to vulnerabilities. Group E stated that individuals within the group could spread private information, either accidentally or intentionally, threatening the security of individual members' personal data. For example, E2 stated that they wanted more transparency knowing what is happening with group messages and commended Snapchat for its increased transparency: *"[I want the] security in knowing what's happening in the group. Knowing who adds and removes who. Knowing who is screenshotting etc.. Snapchat does a good job, [it] increase[s] transparency with [the] other person."* E3 elaborated that messaging platforms like iMessage, do not provide a lot of information about what people are doing with messages they received, *"[With] iMessage, [I] can't tell if someone screenshots.... [I] can't tell what others are doing...."* This finding — that insider threats can be of particular prominence among small, social groups — has been noted in related contexts in the literature. For example, Das *et al.* [7] found that pranks among friends were a common catalyst for behavioral change in S&P, while Matthews *et al.* [25] highlighted ways in which abusive romantic partners violate the digital privacy of their former partners. Existing end-user facing S&P controls, however, do little to acknowledge these insider threats.

*Outsider threats (Groups B, C & D)* are threats from outside of the group. These threats could come from an unknown outsider accessing a shared resource — such as Hulu (group B), or from outsiders accessing devices like laptops and phones (group C). C2 stated that since they stayed logged in to all of their accounts on their laptops and phone, including group messaging accounts, anyone who could access these devices could, in turn, have federated access to all of their accounts and messages, *"I also feel not so secure, but on the level of access through the devices. I stay logged in on both my laptop and phone, so as long as you can get in my phone or laptop, and login, then you can see everything, almost everything. But I stay logged in because I cannot remember all the passwords so it's convenient for me, but also insecure for me, both."*. Technology failure itself, when phone batteries died or when an application did not update fast enough, was a concern in the case of tracking friends' locations (group D). In contrast to insider threats, groups who spoke of outsider threats being their primary concern expressed a sense of accountability for others in the group and desired controls that could help them act on this sense of accountability. This finding echoes calls from prior work, to build new S&P systems that are more *cooperative* — affording people to jointly work towards mutually beneficial S&P outcomes — and *stewarded* — allowing individuals to act for the benefit of others S&P [5, 6].

*Insider-facilitated Outsider Threats (Groups A, F, H & I* are threats from outsiders that are made possible by the actions of insiders — e.g., through negligent practices. These groups experienced threats from inside the group from members having access to shared passwords or physical spaces. For example, H1 stated this sentiment regarding their shared Amazon account, *" For the amazon account because I have my credit card there I have a little bit more concern about that. If the password gets circulated widely, because I have my credit card there so I don't know who's using it and if they somehow... I'm not saying anyone would do it on purpose, but someone mistakenly uses my credit card, then I have to track them down and see who bought what and things like that."* While sharing passwords facilitates distributed access to accounts, the security of this account was only as strong as the group member who did the least to secure the shared password. A parallel situation occurred when each group member shared access to a physical space, as each individual also bore equal responsibility in securing that physical space from outsiders. In this way, group members could become contingent threats if they neglected to adequately secure shared resources against possibly pertinent outside threats.

### Strategies and Attitudes Towards Securing Shared Resources

With a more detailed understanding of *why* groups secured their resources, we codified *how* groups attempted to protect these resources. As suspected, despite resources being collectively owned and shared, strategies for securing access to these resources rested on the security practices of individuals with little group oversight or coordination. Table 3 breaks down strategies that groups employed to maintain the security of their resources. None of our participant groups mentioned the use of existing security controls to explicitly codify or enforce these strategies. While this does not preclude the existence of such infrastructure, none of the authors (some of whom are domain experts) know of any tools that would allow for explicit codification of these strategies. If the technical infrastructure does exist, it is either not easily accessible, largely unknown and/or lacking. For example, when asked about securing resources, members of group D described individual strategies rather than a collective tool that everyone utilized:

D5: We're all responsible for ourselves.
D2: I mean, we all have passcodes on our phones so that locks that.
D4: We also keep our phones secure.
D2: iCloud accounts are locked pretty much, 2-factor authentication for iCloud and all that stuff.
D3: Most of us have the biometric protection too, like touch ID and face ID.

| Group | Strategies |
|---|---|
| A | Regularly updates passwords, has password on device, uses biometric passwords, has 2FA setup, has unknown login alerts, locks devices before stepping away in public space |
| B | Trusted default S&P controls |
| C | Dont add non-group members to group chats |
| D | Has password on device, uses biometric passwords, has 2FA setup, keeps software updated, controls who can see their location, keeps their phones on their person at all time |
| E | Has password on device, don't add non group members to group chats, keeps phones on their person at all times, get permission from group members before adding someone to new resource |
| F | Locks physical spaces, don't add non-group members to group chats, locks devices before stepping away in public space, extra security for physical spaces (cameras, keypads, door auto-lock), don't screenshot conversations |
| G | Keeps software updated, lock items in a secure place |
| H | Regularly updates passwords, locks physical spaces, no extra house keys |
| I | Has password on device, has 2FA setup, extra security for physical spaces (cameras, keypads, door auto-lock), auto lock on phone, verification if too many password attempts, login verification before payment |

**Table 3. Strategies for Securing Shared Resources. Each group protected their shared resources through individual S&P strategies - forming a collective implicit understanding that each member was responsible and accountable for securing their resources. Here we display each group's S&P strategies for securing their resources.**

> D5: And like we don't just give our phones for like other people and they just like go through all of our stuff, it's usually just with ourselves or within our group.

Owing at least partially to the lack of technical infrastructure to help collectively author and enforce shared security policies, groups formed implicit, unspoken agreements and attitudes towards securing shared resources.

*Holding Each Individual Accountable*

In general, our participant groups developed a non-enforceable mutual understanding that necessitated both individual accountability and trust that everyone was doing their best to maintain the security of these resources. Every group agreed that each individual member should be held equally accountable for the security of their shared resources. Group E discussed this viewpoint regarding their group messaging:

> E2: [There's a] level of trust with everyone... [We] hold each other accountable.
> E3: [We] check in with others before adding someone new to the group [and are] each responsible for what stays in the group.

*Social Oversight is Necessary to Improve the Equity and Effectiveness of Group Security*

Due to this implicit, non-enforceable shared responsibility for securing resources, the overall security of many resources reduced down to the security practices of the "weakest link" in the group i.e., the individual who did the least to secure those resources. Participant F1 expressed frustration with the inherent *inequity* and *ineffectiveness* of such a system, *"Yeah it's like for the GroupMe, it kind of sucks that the entire security of the group is tied to everybody's personal habits around, like, being locked in, or their passwords. Like I can have a really great password and I can make sure that I [am] conscientious with leaving devices unlocked but somebody else is lazy and it's like all my work is for nothing."*

Echoing this frustration, Group I discussed how one former group member's failure to follow these implicitly construed S&P norms resulted in a falling out that ultimately led to that individual being ousted from the group. The ousted member was able to make a security-relevant decision on behalf of the entire group (i.e., providing unsupervised access to an outsider) without any form of oversight from the rest of the group. They stated:

> I4: I'll talk about the most awkward one. So we had a roommate sophomore year...and living with her was just too much I guess...we found out she was doing less than legal things, and we were uncomfortable with that and so it was like incredibly awkward....
> I3: And it still is like a little, we are not close to the level of friendship that we were before unfortunately. And then her then boyfriend now fiance would always be over at our apartment and he would sometimes be there when she wasn't there and we thought that was a little...Because he had like her key.
> I2: Yeah, that made us uncomfortable just because he's not technically like our roommate and shouldn't have her key by [school] rules and stuff like that....

This example highlights how the the practices of individual group members combine to form a collective effort in securing shared resources, *but the aggregation function is a "min" rather than a "sum."* Stating this in other words, group security is only as strong as the individual with the weakest security behaviors, which can be inequitable and lead to resentment. Moreover, even if an individual group member invests a significant amount of time and effort into securing the collectively owned resource, this effort by that individual group member can be rendered ineffective by an accidental or intentional action by any other member of the group.

In short, we found that our groups developed implicit and often unspoken rules about S&P policies towards collectively owned resources, and relied on each individual doing their best to maintain the security of the resources with no social oversight. While unobtrusive, this process can lead to inequity, resentment and even loss of group membership in extreme cases of breach.

*Summary: How do groups jointly secure shared resources?*
To summarize, we answered our RQ1 - how do small, social groups (e.g., close friends, class-mates, coworkers, roommates, families) jointly navigate decisions to secure their shared digital resources - and found that groups' resources spanned across five different categories: Digital Media Accounts, Physical Items, Edge Computing Devices, Group Messaging Accounts, and Social Media Accounts. These were shared to maintain a digital connection, for mutual use, and borrowing. We categorized the S&P threats that groups secured their resources against under insider threats, outsider threats, and insider-facilitated outsider threats. Group members often employed their own individual S&P practices that collectively formed to create a mutual S&P strategy to secure against these threats. This resulted in a tacit understanding that each group member was accountable and responsible for the protection of their shared resources. However, groups also expressed frustration with the inherent inefficiency and inequity with a system in which the shared S&P policy towards protected, resources amounted to a patchwork of uncoordinated and invisible individual behaviors.

### RQ2: How Do Groups Affect Individuals' S&P Attitudes?

Prior work suggests that social influences can affect individuals' attitudes and behaviors towards S&P [5, 7], but that S&P are personal topics that are rarely the topic or purpose of social interactions [6, 8]. As small social groups increasingly share and jointly secure collectively-owned digital resources however, the frequency of these S&P-relevant social interactions should increase. Accordingly, we next wanted to explore how group S&P-relevant interactions influenced individual members' attitudes and behaviors towards S&P. To do so, in our supplemental diary and phone study, we asked individuals if they had any S&P-relevant conversations or performed any S&P-relevant actions with their group members in the four-week period following our interviews. We also asked what prompted these conversations and changes.

As suggested by prior work, we found additional evidence reinforcing the presence of an inherent social norm that inhibits discussion of S&P-relevant topics with others [8]. Conversations about S&P occurred only when a widely publicized S&P-relevant news event came to a group member's attention, e.g., the 2018 Facebook data breach in which 50 million Facebook accounts were compromised [36]. Yet, people rarely discussed their individual S&P behaviors, decisions or challenges — often to their own detriment. Indeed, we identified a few missed opportunities for stewardship, in which a problem faced by one group member could have been more easily solved had they been in contact with another. We discuss here our findings for how our groups conversed and thought about S&P, and why these missed opportunities occurred in our groups.

*Conversations About S&P Tended to Focus on the Abstract*
Previous findings by Wiese *et al.* suggests that groups with stronger social bonds (e.g., close friends, roommates, family) tended to converse more freely on S&P relevant topics and were more likely to follow each others' advice than groups with work or study relationships [38]. However, for most groups in our study, conversations about S&P centered around abstract rather than concrete behaviors or strategies. For example, many conversations revolved around major news events about data breaches like the aforementioned 2018 Facebook data breach (groups H,D & I)) [36], 2018 Equifax data breach (group H) [22], and a data breach at the local university some of our participants attended (groups F & C). This finding echoes prior work, which also found that people primarily hear about S&P-relevant breaking news events through friends and family [11]. Another common, abstract topic discussed by groups was how different companies and service providers collected and used personal data (groups I, E, & H).

*Personal and Irrelevant: Reasons Not to Talk About S&P*
During group interviews, when asked about their most recent S&P changes, only six participants (4 members from group A, and 2 members from group D) stated they had talked to another group member about their recent S&P changes. Those who *did* report discussing their recent S&P behaviors with other members in the group tended to share with only certain individuals in the group rather than the entire group.

Similarly, in the diary study, of the 56 instances where participants reported having a thought about S&P, only four were shared with someone else. We found that while no one initially claimed to be hesitant to bring up S&P-relevant conversations with their groups, when prompted further in the group interviews, some recalled that they were hesitant to bring up S&P-relevant events and/or behaviors in two situations.

First, some participants related their hesitancy to bring up a topic due to the personal nature of the issue. For example, when one of their members discussed getting locked out of their Snapchat account, group D had the following exchange:

> D5: ...my Snapchat was, I don't know, something was happening and it was messing up, so I logged out of it and I forgot my passcode to get in so I think I was freaking out with someone...that I can't get back in so then I had to redo, reset my password and everything...
> D4: How'd you feel?
> D5: I felt stupid, usually I remember how to get back in, I can't get back in and I totally forgot my password.... I didn't bring it up to the entire group no, just to like one person.... I didn't feel the need to tell everyone...
> D1: It feels personal.

Second, and more commonly, was participants' notions that if a personal S&P-related event and/or behavior was not specifically relevant to their group's shared resources, there was no need to discuss it. B1, for example, noted that, *"A lot of [my] changes didn't necessarily impact [the] ability to anything* *they'd [the group] have to access.,"* when discussing why she didn't bring up her recent cybersecurity improvements with her group.

Similarly, when discussing why he did *not* share being locked out of his Facebook account and having to change his password, D2 stated: *"I thought that I could just like fix it myself so... I just figured it out on my own, so it's not a high priority on the group conversation ladder."*

This choice *not* to discuss personal S&P events and behaviors suggests that, in general, participants viewed S&P behaviors as a singular transactional experience that had relevance only to themselves in that situation. In other words, participants often viewed S&P experiences that were not explicitly group experiences as having no social or conversational value — they were not trials worth commiserating about, nor challenges that participants took pride in overcoming, nor learned skills worth teaching others. Indeed, a few participants even simply stated they just do not talk about cybersecurity (B4, E2, I), echoing similar findings from prior work [7].

Note, however, that during our interviews, there were a few instances where the act of answering our questions about S&P events led to conversations in which group members learned from one another. Many participants in group D, for example, learned about the Facebook data breach when D2 mentioned they were locked out of Facebook.

> D2: Yeah, so um, my Facebook got locked out, that's kind of why I had to change my passwords if I'm going to be honest, but it's still a routine thing, but yeah, it signed me out of all my Facebook services
> D1: It did that to me too.
> D2: So is that a Facebook thing?
> D3: It got hacked this morning.
> D5: Facebook got hacked?

Likewise, F4 learned about a data breach at school only when F5 mentioned a recent security change he undertook due to the breach:

> F5: I think that the two biggest changes I made is that I started using LastPass for all my passwords. Recently we had a data breach. They sent out emails saying that you are vulnerable... free for an identity protection thing...
> F4: Wait what?
> F5: Yeah you missed the email..

And in the same vein, I2 learned about fingerprint ID for the social payments app, Venmo, when I1 relayed a change he had made after hearing a security story from a friend:

> I1: I got this new phone relatively recently, so it has fingerprint ID on it, so I've been kind of taking advantage of that.... I also added it to Venmo, mostly out of paranoia. Because my roommate was talking about this one story where he heard, which could be completely hearsay, but someone was like, some guy asked another guy, 'Can I borrow your phone to make a call?' or something, and then all of a sudden he had Venmo-ed himself x number of dollars through that guy's phone.
> I3: What?
> I1: So yeah, because of that, he kind of made me paranoid about it, so I added the fingerprint ID to it as well, to make sure it has that extra layer of security, I think [I3] is going to do that right now.
> I3: I think I might have done it, I'm just not sure.
> I2: I didn't know that was a thing you could do.

The group interviews were an unnatural forcing function for S&P conversations in which group members shared relevant, actionable advice with one another. These conversations may have never occurred outside of our group interviews. We suspect that there are many more missed opportunities for learning and stewardship as a result of this view of personal S&P events as being singular transactional experiences.

#### *Summary: How do group interactions affect individual S&P attitudes and behaviors?*

In general, we found that group interactions around S&P were rare and avoided. Moreover, when they did occur, they tended to focus on S&P in the abstract — about large data breaches or breaking news events. Individuals rarely brought up their own S&P behaviors with their groups because they found them to be personal and irrelevant to the group. This unilateral focus on abstract breaking news events about S&P can contribute to a sense of defeatism or nihilsm: that no matter what one does, one can never be safe [11]. Moreover, this finding suggests that individuals largely view S&P behaviors as singular transactional experiences that affect only themselves at that time, and that they hold no social or conversational value. Yet, when our interview questions forced groups to discuss individual S&P behaviors, we saw a number of instances in which these individual behaviors sparked animated conversations and learning experiences. We suspect, therefore, that there are many missed opportunities for learning and stewardship due to the *absence* of S&P-relevant group interactions.

## DISCUSSION

As computing becomes increasingly social, the S&P controls that we use to protect our collectively owned and shared resources must be updated to reflect this new reality. The high-level upshot of our work is that existing S&P controls are inadequate for small, social groups. Indeed, in our effort to understand how groups shared and secured their resources, and how they influenced each other's S&P behaviors, we found that our groups formed implicit, unspoken rules around security that were inequitable and unenforceable. Groups desired individual accountability, but the specifics of what was expected and how it would be enforced were unclear. This collective responsibility put the onus to protect the S&P of the group and the resource on each individual member, yet the protection of the group as a whole reduced down only to the S&P practices of the individual who did the least. Given groups' hesitation to discuss S&P topics with one another, the inefficiencies and inequities with the status quo does not come to a head until something goes wrong: e.g., a breach occurs, or a group member violates the implicit rules egregiously or often enough to lose membership. We next discuss design implications for group S&P controls that better supports small, social groups in expressing and enforcing mutually agreeable S&P decisions for their protected, shared resources.

### S&P Controls That Facilitate Group Stewardship

Our findings reveal that one of the biggest vulnerabilities to group resources were insider threats and insider-facilitated threats (e.g., threats made possible or likely by group members with the weakest S&P practices). We argue that there is a need for S&P tools and systems that allow group members with higher S&P awareness, motivation and knowledge to act as *stewards* for more vulnerable members. These systems should foster teachable moments in which more experienced group members teach more vulnerable members how to make better S&P decisions. Prior work suggests that social learning and intervening during teachable moments are among the most effective ways to improve S&P behaviors [8, 21]. This active facilitated stewardship should help reduce the occurrence of insider and insider facilitated threats and improve the S&P of groups shared resources.

### A Context-Aware Shared Pool of S&P Experiences

Groups rarely discussed S&P topics with one another, and when they did, these topics revolved around abstract events and concepts. However, our interviews revealed that when conversations occurred around more concrete and personal experiences and behaviors, these anecdotes afforded opportunities for S&P growth in others. In parallel, our findings also suggest that a key reason that groups share digital data and resources is to maintain a persistent digital connection with other group members. There is an opportunity to develop tools that both provide groups with a novel outlet to maintain a digital connection while improving shared S&P knowledge by simplifying the process of sharing one's recent S&P behaviors and experiences. One such hypothetical system might detect an individual's positive S&P behaviors and offer them the opportunity to easily share this positive behavior in a group channel—perhaps with context-specific constraints. For example, after one group member registers for 2FA on their email, they might be presented with a just-in-time prompt to inform other group members of this behavior the next time those group members log in to their emails. This low overhead dispersal of concrete knowledge and experience should help level the S&P knowledge of group members.

### Systems for Social Governance of Shared S&P Policies

Groups desire more social oversight in protecting their resources, but do not, generally, want to discuss S&P-topics with one another. How can one both create a system that increase S&P-related interactions by affording greater oversight, but that also respects group members' desires to not want to discuss S&P with one another? We argue that designers should explore creating S&P systems that allow individual group members to specify their ideal policies for a shared resource, and then only have them address conflicts in their ideal policies through a joint process. Such a system could afford oversight, transparency and enforce-ability without requiring constant S&P related interaction. This process might, for example, be "democratic", where each group member can vote on proposed policies. While a "democratic" system of governance may not be appropriate for all groups, it should serve as a good starting point to explore alternatives that are better suited to groups with different social dynamics (e.g., coworkers vs. parents and children vs. roommates). We caution, however, that such tools should be designed and evaluated carefully—explicit codification of shared access control policies could potentially have negative social ramifications (e.g., if one group member is deemed to have reduced access).

## LIMITATIONS

As with any empirical study, ours has limitations that are worth noting while interpreting our findings. We discuss the most pertinent such limitations here.

*Recruiting:* We had difficulty recruiting groups who were able to come in, as a collective, to do an interview. Even though we recruited our target number of participants, our data only represents the groups we interviewed and are not fully representative of the different group dynamics and relationships that exist. However, even if preliminary, our findings are still important for understanding how small social groups behave and interact regarding the S&P of their shared resources, and how current S&P controls do not meet their needs. We also identified design implications that more broadly emphasizes the need to bridge this social-technical gap.

*Representative sample:* The majority of our groups represent student relationships and dynamics, therefore we have limited data on groups of middle-aged and older people, and in particular groups of colleagues and families. This might be due to time conflicts as these groups would be more pressed for time due to job and family requirements. Perhaps there was lack of motivation for these groups as well.

*Diary study:* Lastly, we found participants were underreporting in the diary study. We remedied this by utilizing follow up phone interviews to ascertain more detailed explanations of answers to the questionnaires.

## CONCLUSION

In this paper, we present the first exploration of how small groups of socially connected individuals (e.g., close friends, families, roommates) jointly navigate decisions to secure shared digital resources. Through a multi-method qualitative study conducted over seven months, we found that: (i) strategies for securing these shared resources hinged primarily on implicit agreement and individual accountability; and, (ii) that our groups rarely communicated about S&P which, in turn, led to missed opportunities for security stewardship. More generally, we found that existing S&P controls failed to meet the nuanced social requirements of our participant groups, and we identified a number of design opportunities to bridge these social-technical gaps. In brief, as we delve deeper into an era of social computing, notions of digital resource ownership are often complicated through both shared and social uses of digital resources. Our research highlights a growing need for the design of cybersecurity and privacy controls that better support the needs of small, social groups.

## ACKNOWLEDGMENTS

Thanks to Jason Paul, Amy Bruckman, Gregory Abowd, Rosa Arriaga for their input and assistance. This research was generously supported, in part, by the National Science Foundation through grant SaTC-1755625.

# REFERENCES

[1] Mark S. Ackerman. 2000. The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility. *HumanâĂŞComputer Interaction* 15, 2-3 (sep 2000), 179–203. DOI: http://dx.doi.org/10.1207/S15327051HCI1523_5

[2] Steve Berry, Steven Fazzio, Yongyi Zhou, Bethany Scott, and Luis Francisco-Revilla. 2010. Netflix recommendations for groups. *Proceedings of the American Society for Information Science and Technology* 47, 1 (nov 2010), 1–3. DOI: http://dx.doi.org/10.1002/meet.14504701402

[3] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (jan 2006), 77–101. DOI: http://dx.doi.org/10.1191/1478088706qp063oa

[4] A. J. Bernheim Brush and Kori M. Inkpen. 2007. Yours, Mine and Ours? Sharing and Use of Technology in Domestic Environments. In *UbiComp 2007: Ubiquitous Computing*. Springer Berlin Heidelberg, Berlin, Heidelberg, 109–126. DOI: http://dx.doi.org/10.1007/978-3-540-74853-3_7

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

[6] Sauvik Das, Laura A Dabbish, and Jason I Hong. 2019. A Typology of Perceived Triggers for End-User Security and Privacy Behaviors. In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS '19)*. 19.

[7] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. 2014a. USENIX Association Tenth Symposium On Usable Privacy and Security 143 The Effect of Social Influence on Security Sensitivity. In *12th USENIX security symposium.* USENIX Association, 143–157. https://www.usenix.org/system/files/conference/soups2014/soups14-paper-das.pdf

[8] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2014b. Increasing Security Sensitivity With Social Proof: A Large-Scale Experimental Confirmation. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14)*. ACM, New York, NY, USA, 739–749. DOI: http://dx.doi.org/10.1145/2660267.2660271

[9] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2015. The Role of Social Influence in Security Feature Adoption. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing - CSCW '15*. 1416–1426. DOI:http://dx.doi.org/10.1145/2675133.2675225

[10] Sauvik Das, Gierad Laput, Chris Harrison, and Jason I Hong. 2017. Thumprint: Socially-inclusive local group authentication through shared secret knocks. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 3764–3774.

[11] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I. Hong. 2018. Breaking! A Typology of Security and Privacy News and How It's Shared. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 1, 12 pages. DOI: http://dx.doi.org/10.1145/3173574.3173575

[12] Paul Dourish and Ken Anderson. 2005. Privacy, Security ... and Risk and Danger and Secrecy and Trust and Morality and Identity and Power: Understanding Collective Information Practices. *ISR Technical Report* UCI-ISR-05-1 (2005), 1–19.

[13] Serge Egelman, A.J. Bernheim Brush, and Kori M. Inkpen. 2008. Family accounts. In *Proceedings of the ACM 2008 conference on Computer supported cooperative work - CSCW '08*. ACM Press, New York, New York, USA, 669. DOI: http://dx.doi.org/10.1145/1460563.1460666

[14] Serge Egelman and Eyal Peer. 2015. Scaling the Security Wall. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*. ACM Press, New York, New York, USA, 2873–2882. DOI: http://dx.doi.org/10.1145/2702123.2702249

[15] Rosta Farzan, Laura A. Dabbish, Robert E. Kraut, and Tom Postmes. 2011. Increasing Commitment to Online Communities by Designing for Social Presence. In *Proceedings of the ACM 2011 Conference on Computer Supported Cooperative Work (CSCW '11)*. ACM, New York, NY, USA, 321–330. DOI: http://dx.doi.org/10.1145/1958824.1958874

[16] Shirley Gaw, Edward W Felten, and Patricia Fernandez-Kelly. 2006. Secrecy, flagging, and paranoia. In *Proceedings of the SIGCHI conference on Human Factors in computing systems - CHI '06*. ACM Press, New York, New York, USA, 591. DOI: http://dx.doi.org/10.1145/1124772.1124862

[17] Carlos A Gomez-Uribe and Neil Hunt. 2016. The netflix recommender system: Algorithms, business value, and innovation. *ACM Transactions on Management Information Systems (TMIS)* 6, 4 (2016), 13.

[18] Maia Jacobs, Henriette Cramer, and Louise Barkhuus. 2016. Caring About Sharing. In *Proceedings of the 19th International Conference on Supporting Group Work - GROUP '16*. ACM Press, New York, New York, USA, 235–243. DOI: http://dx.doi.org/10.1145/2957276.2957296

[19] William Jang, Adil Chhabra, and Aarathi Prasad. 2017. Enabling multi-user controls in smart home devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*. ACM, 49–54.

[20] Joseph 'Jofish' Kaye. 2011. Self-reported password sharing strategies. In *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11*. ACM Press, New York, New York, USA, 2619. DOI: http://dx.doi.org/10.1145/1978942.1979324

[21] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. 2010. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)* 10, 2 (2010), 7.

[22] LifeLock. 2017. Equifax Data Breach Affects Millions of Consumers. HereâĂŹs What to Do. (2017). https://www.lifelock.com/learn-data-breaches-equifax-data-breach-2017.html Accessed: 2019-04-03.

[23] Alice E Marwick and Danah Boyd. 2014. Networked privacy: How teenagers negotiate context in social media. *New media & society* 16, 7 (2014), 1051–1067.

[24] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. "She'll just grab any device that's closer". In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*. ACM Press, New York, New York, USA, 5921–5932. DOI: http://dx.doi.org/10.1145/2858036.2858051

[25] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. 2017. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 2189–2201.

[26] Michelle L. Mazurek, J. P. Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, Richard Shay, Kami Vaniea, Lujo Bauer, Lorrie Faith Cranor, Gregory R. Ganger, and Michael K. Reiter. 2010. Access Control for Home Data Sharing: Attitudes, Needs and Practices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, New York, NY, USA, 645–654. DOI: http://dx.doi.org/10.1145/1753326.1753421

[27] Leysia Palen and Paul Dourish. 2003. Unpacking "privacy" for a networked world. In *Proceedings of the conference on Human factors in computing systems - CHI '03*. ACM Press, New York, New York, USA, 129. DOI: http://dx.doi.org/10.1145/642611.642635

[28] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, and Laura Dabbish. 2018. Share and Share Alike? An Exploration of Secure Behaviors in Romantic Relationships. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*. https://www.usenix.org/conference/soups2018/presentation/park

[29] Keith Patrick and Fefie Dotsika. 2007. Knowledge sharing: developing from within. *The Learning Organization* 14, 5 (2007), 395–406. DOI: http://dx.doi.org/10.1108/09696470710762628

[30] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories As Informal Lessons About Security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. ACM, New York, NY, USA, Article 6, 17 pages. DOI: http://dx.doi.org/10.1145/2335356.2335364

[31] 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. DOI: http://dx.doi.org/10.1109/SP.2016.24

[32] Yuqing Ren, F. Maxwell Harper, Sara Drenner, Loren Terveen, Sara Kiesler, John Riedl, and Robert E. Kraut. 2012. Building Member Attachment in Online Communities: Applying Theories of Group Identity and Interpersonal Bonds. *MIS Quarterly* 36, 3 (2012), 841–864. http://www.jstor.org/stable/41703483

[33] Kai Sassenberg. 2002. Common bond and common identity groups on the Internet: Attachment and normative behavior in on-topic and off-topic chats. *Group Dynamics: Theory, Research, and Practice* 6 (03 2002), 27–37. DOI: http://dx.doi.org/10.1037/1089-2699.6.1.27

[34] Saul Shiffman, Arthur A. Stone, and Michael R. Hufford. 2008. Ecological Momentary Assessment. *Annual Review of Clinical Psychology* 4, 1 (2008), 1–32. DOI: http://dx.doi.org/10.1146/annurev.clinpsy.3.022806.091415 PMID: 18509902.

[35] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. 2007. Password sharing. In *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '07*. ACM Press, New York, New York, USA, 895. DOI: http://dx.doi.org/10.1145/1240624.1240759

[36] TechCrunch. 2018. Everything you need to know about FacebookâĂŹs data breach affecting 50M users. (2018). https://techcrunch.com/2018/09/28/everything-you-need-to-know-about-facebooks-data-breach-affectin Accessed: 2019-04-03.

[37] Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10*. ACM Press, New York, New York, USA, 1. DOI: http://dx.doi.org/10.1145/1837110.1837125

[38] Jason Wiese, Patrick Gage Kelley, Lorrie Faith Cranor, Laura Dabbish, Jason I. Hong, and John Zimmerman. 2011. Are you close with me? are you nearby?. In *Proceedings of the 13th international conference on Ubiquitous computing - UbiComp '11*. ACM Press, New York, New York, USA, 197. DOI: http://dx.doi.org/10.1145/2030112.2030140