"How Do You Not Lose Friends?": Synthesizing a Design Space of Social Controls for Securing Shared Digital Resources Via Participatory Design Jams

Eyitemi Moju-Igbene, Hanan Abdi, Alan Lu,
and Sauvik Das, *Georgia Institute of Technology*

https://www.usenix.org/conference/usenixsecurity22/presentation/moju-igbene

This paper is included in the Proceedings of the
31st USENIX Security Symposium.

August 10–12, 2022 • Boston, MA, USA

978-1-939133-31-1

Open access to the Proceedings of the
31st USENIX Security Symposium is
sponsored by USENIX.

"How Do You Not Lose Friends?": Synthesizing a Design Space of Social Controls for Securing Shared Digital Resources Via Participatory Design Jams

Eyitemi Moju-Igbene
Georgia Institute of Technology

Hannan Abdi
Georgia Institute of Technology

Alan Lu
Georgia Institute of Technology

Sauvik Das
Georgia Institute of Technology

Abstract

Digital resources (streaming services, banking accounts, collaborative documents, etc.) are commonly shared among small, social groups. Yet, the security and privacy (S&P) controls for these resources map poorly onto the reality of shared access and ownership (e.g., one shared Netflix password for roommates). One challenge is that the design space for social S&P controls remains unclear. We bridged this gap by engaging end-users in participatory design workshops to envision social solutions to S&P challenges common to their groups. In analyzing the generated ideas and group discussions, we identified four design considerations salient to social S&P controls: social transparency; structures of governance; stakes and responsibility; and, promoting pro-group S&P behaviors. Additionally, we discovered trade-offs and challenges that arise when designing social S&P controls: balancing group security versus individual privacy; combating social friction; mitigating social herding behaviors; and, minimizing coordination costs.

1 Introduction

Many digital resources — valuable, computationally accessible devices and accounts — are collectively owned or shared by small groups of socially-connected individuals [52] (e.g., Netflix accounts shared among friends, bank accounts shared among families, documents shared among colleagues). These shared digital resources are increasingly abundant, and must be secured in a manner that preserves access to individuals in the group while also preventing access to those outside of the group. While a simple design constraint in theory, prior work suggests that many social groups have trouble negotiating this trade-off with existing security and privacy (S&P) controls [5, 19, 34, 44, 52].

The emerging discipline of social cybersecurity suggests that part of the challenge is that existing S&P controls are non-social: they are designed for individual use and often assume digital resources are owned by individuals [6, 11–14]. Based on this prior work, we hypothesized that it should be possible to create social S&P controls for shared digital resources that better map onto models of collective ownership and access. However, the design space of such social S&P controls for shared digital resources remains unclear. Our research aims to develop this design space from the perspective of the end-user by addressing the following research questions:

- **RQ1:** What are the key design dimensions for implementing social S&P controls for shared digital resources?
- **RQ2:** What are the trade-offs between these design dimensions and how might these trade-offs introduce new challenges?

To answer these questions, we conducted in-person[1] participatory design workshops with 11 groups of 3-5 participants (n = 43), each tasked with imagining novel social S&P controls for shared digital resources. Participants were assigned to a social group that aligned with the type they share resources with in their personal lives (e.g., roommates). Most groups included at least one individual with prior experience in design or engineering. We observed what S&P and social needs these participant groups deemed important and what trade-offs they were willing to make to meet those needs. We qualitatively analyzed the observations, prototypes, and exit surveys results through an iterative coding process. Importantly, our goal was to use the ideas generated by participants as *lenses* to understand desirable properties for social S&P controls — thus, we do not espouse or specifically recommend any individual idea generated by our participant groups.

We found four key design dimensions to consider for social S&P controls for shared digital resources: *social transparency*, or the ability for the group to observe and monitor individual group members' actions; *structures of governance*, or how groups collectively make S&P-relevant decisions about a

[1] These sessions occurred in the U.S. in Jan/Feb 2020, before remote participation recommendations were instituted as a result of the COVID-19 pandemic.

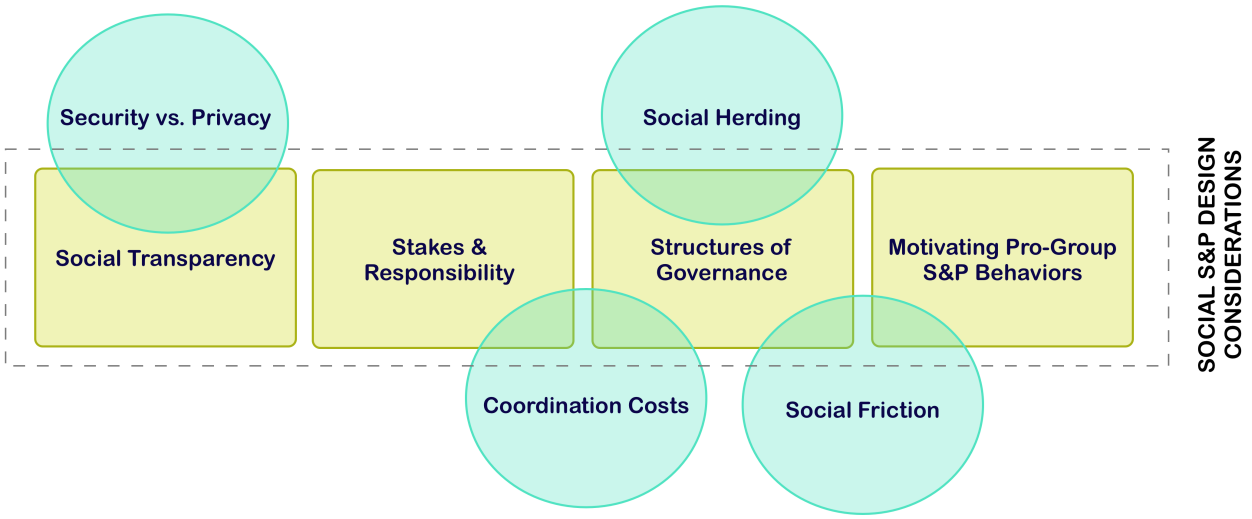


Figure 1: The design space of social cybersecurity and privacy controls for shared digital resources we uncovered in our study. We identified four key design dimensions and intersecting trade-offs.

shared digital resource; *stakes and responsibility*, or methods to fairly distribute responsibility for the S&P of the shared resource; and, *promotion of pro-group S&P behaviors*, or methods to incentivize behaviors beneficial to group S&P (and to punish poor ones).

We also identified trade-offs that arose between these dimensions when designing social S&P controls for shared digital resources. These trade-offs included: balancing an individual's desire for privacy against the group's desire for social transparency; mitigating herding behavior; alleviating social friction; and, accounting for coordination costs.

We conclude by reflecting on the ideas participants generated, the relationship between group type and the design dimensions we uncovered, the need to anticipate issues with access and power, and the feasibility of implementing ideas for social S&P controls using existing technologies.

2 Related Work

Our work is informed by and extends a number of open threads of research spanning social cybersecurity theory and systems, as well as participatory design jams as a research method.

2.1 Social S&P for Shared Digital Resources

Ackerman [1] argued that there is a *social-technical gap* between what is technically feasible and what is socially required of social computing systems. As an example, he cited the Platform for Privacy Preferences (P3P), contending that the privacy controls afforded by P3P did not adequately support the social nuance necessary in online content sharing. This social-technical gap is still evident in many modern end-user S&P controls [52].

DiGoia and Dourish [17] proposed "social navigation" as a model for usable security, in which they proposed a user interface design in which users would see implicit social signals of how others have configured their S&P controls. Singh et al. [43] explored households' password sharing practices for bank accounts, finding that the practice was commonplace despite being discouraged, and argued for more social design in password systems. Watson et al. interviewed nine small social groups to explore how S&P groups navigated securing shared resources [52]. They found that strategies for securing shared resources were often implicit and unspoken. In turn, they found that the lack of technical infrastructure to support shared decision making, oversight, and enforcement strategies could lead to frustration, inequity, and ineffectiveness.

Following a series of empirical results exploring the relationship between social influence and end-user S&P behaviors [11–14, 16], Das introduced the concepts of observability, cooperation and, stewardship as social dimensions relevant to the design of effective social S&P systems [10]. Observable S&P systems should be visible to selected others to encourage social proof. Cooperative S&P systems should enlist collectives acting in concert for mutual S&P benefit. Stewarded S&P systems allow individuals to act on behalf of and/or in benefit to others [10].

Some prior work has also explored designing, implementing, and evaluating such systems. For example, Toomim et al. proposed a novel social access control mechanism for online photos that afforded access to potential viewers based on shared social knowledge [49]. Egelman et al. explored "Family Accounts," or shared accounts that all members of a family could utilize to access shared resources on a collec-

tively owned computer [19]. Das et al. introduced Thumprint, a social authentication mechanism that authenticates and identifies individual group members through a shared secret knock [15].

Although tools have been implemented for specific S&P scenarios, the foundational design dimensions have not yet been formally explored and the dangers of group-based information management are still present. Similar to Lampinen et al.'s research on Social Network Systems, users of shared digital resources cannot control what other group members disclose about their shared space and this sets up a challenge for introducing preventative measures for managing sensitive information disclosure [28].

In sum, these prior works motivate the need for more privacy and cybersecurity design considerations when creating such systems for shared digital resources. We contribute to this thread of research by addressing the call for formally exploring the design space of social cybersecurity systems for digital resources shared by small, social groups.

2.2 Group Sharing of Digital Resources

Prior studies have modeled the sharing of digital resources and resources between individuals. Whitty et al. investigated individuals sharing passwords and found that younger people share passwords more often than older people and that perseverance was a significant factor in sharing impulsively [54]. Kaye found that people regularly share passwords within their socially connected groups [26]

Previous work has recognized major themes relating to how and what technology is shared by different social groups, specifically among family, colleagues, and romantic partners. With families, studies focus on privacy concerns over personalized sharing due to the higher levels of trust between members [5]. Mateas et al. discovered domestic ubiquitous computing technology is usually found in a shared space like a family room and kitchen as opposed to a more remote area such as a workspace [32]. Additionally, Matthews et al. discovered household members would commonly share accounts, devices, and even mobile phones due to mutual need, limited resources, and convenience despite the fact that these devices were considered "personal" [33]. On the other hand, research shows coworkers are strongly affected by autonomy when sharing resources [27, 37]. A perceived level of self-efficacy improves knowledge sharing behaviors in salespeople-coworker relationships and affects employee task performance. With romantic relationships, the types of digital resources shared evolves as the relationship evolves [40] with Jacob et al. classifying this information into public, tailored and personal content [24]

Different social groups will differ in expectations with respect to securing sharing digital resources. Our work models how sharing practices in different social groups affects preferences for social S&P controls for shared digital resources.

2.3 Participatory Design Jams

The inclusion of prospective users into the design process can help bridge the knowledge gap between designers and end-users [4, 38]. In design jams, participants engage in acts of making, storytelling, and enacting to imagine a desired future practice [4]. Design jams are used to various ends, including product idea innovation [25, 31], internal problem solving [8], design pedagogy [45, 51], and as a research methodology [2, 30, 36, 39, 42]. One of the main objectives of a design jam is to engender design representations—such as mockups and storyboards—that help participants communicate their ideas in a concrete manner [50].

Recent studies have leveraged participatory frameworks for usable security and privacy design. Mir et al. demonstrate how a participatory framework can be used to enable vulnerable communities to articulate their concerns and expectations around privacy and data use [38]. Chouhan et al. conducted participatory design jam-esque activities in which participant groups prototyped ideas to better inform individual S&P decisions and behaviors as a form of community oversight [6]. More broadly, end-user participation has been noted to be valuable in the development process for groupware (i.e. applications to support group work [41]).

Our research aims to address fundamental design questions for building usable social cybersecurity systems. Stolterman found at human–computer interaction (HCI) conferences, designs of new forms of interactivity are usually based on earlier *conceptual evaluations* exploring a *concept-driven approach* with a focus on theoretical improvements [47]. It's also important to understand how non-experts design for themselves in order to guide designers into building accessible and robust solutions. Yang et al. describes design implications for building ML tools grounded in non-experts as *sensitizing concepts*, which provide possibilities for a new design space and offers a starting place for future design innovation [55]. Our design jams also yield several design implications for future small group cybersecurity controls.

3 Methodology

In our study, we used participatory design jams to elicit the social and contextual considerations that small, social groups find important in securing shared digital resources, as demonstrated through the ideas participants generated. We elected to use participatory design jams to elicit these ideas from participants as opposed to, e.g., interviews or questionnaires, so that participants could collaboratively think through, refine and discuss their ideas in the process of operationalizing how the idea might work in practice. As has been argued by prior work, the mere act of design can synthesize otherwise inaccessible knowledge [58]. Moreover, by recruiting both participants with design knowledge and those with experiential knowledge (i.e., those who navigate securing shared resources in small,

social groups in their real lives), we ensured that both technical expertise and lived end-user experiences were factored into the conceptual ideas participants produced. Nevertheless, given the rushed nature of the task, we emphasize that the specific concept designs presented are not our contribution — our contribution, rather, is an intellectual analysis of the concept designs produced in order to synthesize high-level design considerations, and the trade-offs therein, for social S&P controls for small groups.

3.1 Recruitment, Ethics & Compensation

We recruited people for in-person participatory design jam workshops through a combination of online advertisements (using Nextdoor, Slack, and Craigslist) and posting flyers around a metropolitan area in the Southeast United States. To ensure that our participant pool had a baseline level of familiarity with the problem space, we required potential participants to have either shared a digital protected resource in a small socially group (colleagues, roommates, family, or friends) or self-identify as a designer and/or developer. We verified eligibility through an online screening survey. The extent of security expertise was not screened as we intended to explore the design space for everyday users and not specifically security experts. Designers and developers were recruited for design jams to stay focused and groups would have baseline design process experience. Our protocol was reviewed and approved by an Institutional Review Board.Each participant signed a group image license form along with a consent form informing them about the data collected and how it would be used. Participants received $25 in compensation in addition to snacks during the session.

3.2 Participants & Group Assignment

We recruited 43 participants[2] split across the four in-person workshops. Participants were aged 18 to 54 years old, included more males (60%) than females (40%) and identified as Asian - 40%, White - 27.9%, Black - 20.9%, Hispanic or Latino - 2%, Other - 2%, Preferred not to say - 7%. Education level was varied with High School - 5%, Some College - 37%, Bachelors - 19%, Masters - 30%, Postgraduate - 5%, Professional - 5%. To ensure participant groups had the necessary experience and expertise to engage meaningfully in the design jam, each group consisted of at least one self-identified designer or developer[3]. Moreover, participants were assigned to their self-identified social group from their screening survey as closely as possible (e.g., people who reported sharing digital resources with roommates were assigned to the roommate group in the design jam). However, some participants may have been assigned to a different social group. Group types are detailed in Table 1.

[2]Participant demographics are further detailed in the appendix

[3]Two groups did not have a designer or developer

Group	Group Type	N
A	Family	4
B	Roommates	4
C	Friends	3
D	Roommates	3
E	Colleagues	3
F	Roommates	4
G	Colleagues	4
H	Family	4
I	Colleagues	4
J	Family	5
K	Friends	5

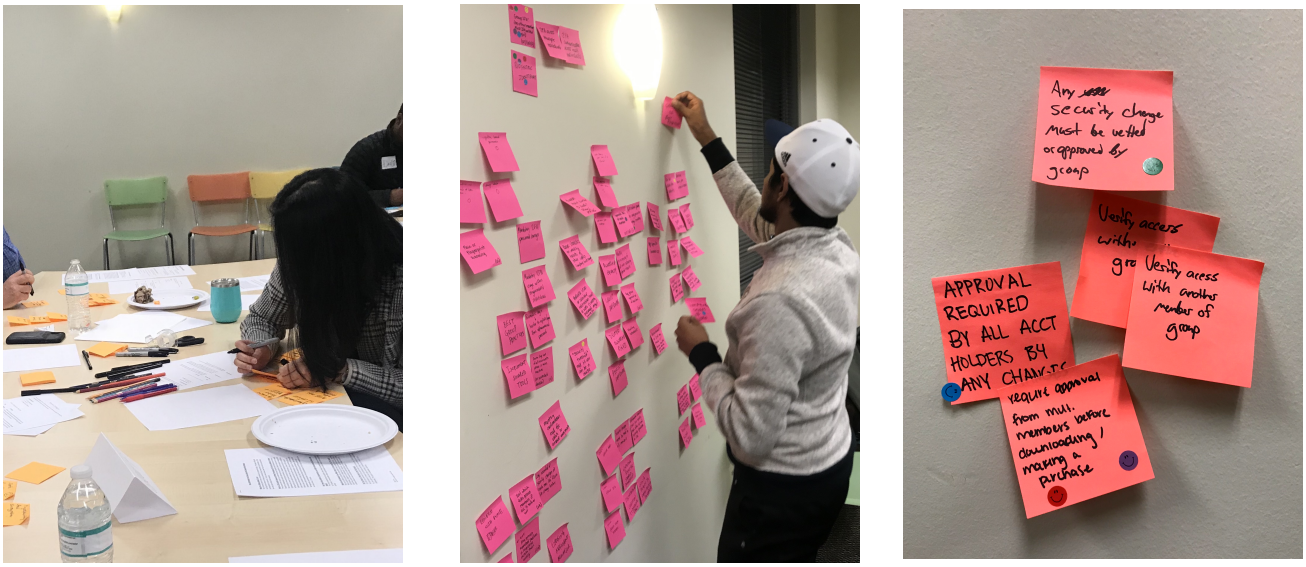
Table 1: Group Types (N = 43). Each workshop had 3-4 groups, each representing a type a socially connected group, and consisted of 3-5 participants per group

3.3 Procedure

We video recorded and transcribed the workshops, each of which lasted around 120 minutes, including a break, and consisted of five phases.

Orientation (15 min.) Three researchers moderated the design jam session. They started by asking participants' how they shared and secured their shared digital resources to get participants thinking about security. Because the design jam was centered around everyday use cases, the participants were not security experts. The researchers introduced core cybersecurity principles and encouraged them to think about ways social influence (e.g., observability, inclusiveness and stewardship [10]) could affect their security behaviors. Additionally, they were given an introduction to core S&P and social design principles (e.g., definitions of S&P, types of threats that groups can encounter [52]) in order to establish a baseline level of familiarity with the broader design space. The orientation was meant to provide groups with a shared foundation of terminology so that the conversation stayed focused and non-experts could feel empowered to contribute. The specific security principles explained can be found in the Appendix. Participants were then introduced to their assigned social group.

Brainstorming & Convergence (30 min.) Participants next engaged in both independent and collaborative brainstorming sessions as illustrated in Figure 2. Participants started by independently brainstorming, on post-it notes, social S&P controls suited to their assigned social groups. We then asked participants to come together as a group to discuss their individual ideas and engage in session of collaborative brainstorming. Groups voted on their best idea to prototype in the next phase. During this phase, we used observation notes



(a) individual brainstorming (b) group brainstorming on the wall (c) dot voting on favorite ideas

Figure 2: Brainstorming process: a) Participants were first guided in an individual brainstorming activity; b) groups then pooled all of their individual ideas together, discussed them, and added any resulting new ideas; c) finally, each participant was given three stickers to dot vote on their favorite idea.

and sticky notes to record each idea groups brainstormed as well as intra-group discussions about their ideas.

Prototyping (30 min.) Third, each social group had 30 minutes to create a storyboard or low-fidelity prototype of the idea they selected during the brainstorming session. To facilitate this process, we provided participants with several drawing mediums such as paper, markers, scissors etc. During this phase, we recorded intra-group discussions on how to design the storyboard or prototype.

Inter-group Presentation & Discussion (25 min.) Fourth, the groups presented their finalized product to everyone in the workshop. They described the problem scenario, which S&P principles their final prototype focused on, and the storyboard or prototype itself. Following the presentations, participants discussed and explored the design implications of each group's solution. During this phase, we video-recorded the presentations and inter-group discussions on each group's final product.

Exit Survey (5 min.) Finally, participants filled out an individually administered exit survey, in which they described which group's solution within the workshop was most relevant to their personal experience as well as what scenarios they would use said idea.

3.4 Data Analysis

We analyzed the data produced—video transcripts of demos and discussions, observation notes of brainstorming, and open-ended responses to questions in the exit survey—using an iterative, open coding process [7]. Two researchers jointly open coded a subset of the data and created an initial set of high level axial codes. Using these codes, they independently coded all the data, including the initial subset. Finally the researchers jointly iterated on their independent code assignments and resolved disagreements through discussion until they had the final codebook. This codebook was grouped into the larger themes we discuss in our results. We did not calculate inter-rater reliability (IRR) as recent work suggests that IRR can be detrimental to work in which code generation is a part of the analysis (as was the case in this work) [35].

The objective of our analysis was to use the ideas generated by participants as *lenses* to understand desirable properties for social S&P controls and the trade-offs therein. Thus, it is important to note that we do *not* necessarily recommend any individual idea generated by our participant groups — some of the generated ideas may be ill-considered if implemented. However, the act of instantiating ideas (e.g., through building prototypes, storyboards, and co-design) can synthesize generalizable design knowledge [58] — we consider this synthesis, and not the specific ideas, to be our core intellectual contribution.

4 Results

We uncovered four key design dimensions to consider in social S&P controls for shared digital resources, along with four key trade-offs and challenges that arise in considering these design dimensions. We provide a broad overview of how different group types embodied different design considerations in their final prototypes in Figure 3. Table 2 lists and describes the final prototype produced by each group. As a reminder, we do not necessarily recommend that these *specific* ideas be implemented — rather, we use the ideas participants generated as lenses through which we might uncover desirable design dimensions and properties for social S&P controls from the end-user perspective.

4.1 RQ1. Key Design Dimensions for Social S&P Controls

4.1.1 Social Transparency

The first design consideration is increased social transparency; that is, the ability to know what others in the group are doing or have done with the shared digital resource.

The need for social transparency is a finding that expands on a rich body of research in CSCW calling for socially translucent systems (i.e., mechanisms that "support coherent behavior by making participants and their activities visible to one another") [22, 48, 52] and observability in social cybersecurity [13]. However, social transparency is rarely considered in the design of S&P controls — even for systems and resources that are commonly shared. Our results provide compelling evidence that it is time to strengthen the bridge between CSCW systems design and usable S&P.

Erickson et al. define three properties of socially translucent systems: visibility, awareness, and accountability. Participants leveraged visibility most when designing their social S&P controls.

Visibility Visibility describes the extent to which one can readily perceive socially significant information. Participant groups most frequently suggested ideas that would allow them to perceive other group members' account activity. Ideas included real-time notifications of shared usage (e.g., group members' login attempts, downloads, purchases, transactions, passwords changes, account settings changes) and revision histories.

These systems were also sometimes envisioned to detect and report group behaviors that could be deemed problematic, such as taking and forwarding screenshots of confidential group information. Several groups described systems that could auto-detect which group members' activities posed significant security threats and alerted other group members with labels such as "pertinent" or "emergency."

Many of the concerns supporting the need for visibility arose out of concern for insider-facilitated outsider threats [52], as demonstrated by Group B's (Roommates) solution that allows users to view a history of login attempts and their originating devices: "*You'd be able to say like, this was me or us, or this wasn't us...I guess it's solving the issue when people in a shared account give passwords out and they shouldn't.*" (B3)

However, not all desires for visibility were fueled by precautions of misconduct. Being able to see group members' activity also served as a way to monitor and correct group members. For instance, a member of Group J (Family) talked about how "*it could tell me...grandma downloaded 18 things.*"(J2). In this way, the participant envisions observing the missteps of an inexperienced member and helping to correct them. This also confirms prior work showing families are open to personalized sharing due to higher levels of trust [5].

At its root, the need for social transparency addresses the loss of control a user may experience after sharing resource access with other independent actors and compensates for this by instituting hypervigilance.

4.1.2 Structures of Governance

The second design consideration was structures of governance for shared S&P controls. We found that a group's decision-making reflected existing authoritative hierarchies. These hierarchies manifested in how groups defined their relationship dynamic or how members considered ownership of their shared resources. These structures of governance fell into one of two categories: egalitarian and hierarchical. While it is perhaps unsurprising that different groups prefer different structures of governance, we note that existing S&P controls offer little support for modifying governance structures for shared resources — the assumption is often that there is one un-elected owner in charge (e.g., access control to photos on Facebook), or that anyone with access has equal control (e.g., shared access to a Netflix account).

Egalitarian Governance In egalitarian governance, all group members have equal power and say. Decisions regarding security and access require either unanimity, a majority, or any member to assent without giving any individual special privileges. When asked if their group type influenced their design, a participant from a roommate group responded, "*I would say yes, because everybody in our scenario is on an equal playing field and they're all coming together for a shared goal*" (D1). While other group types discussed elements of egalitarian structures during brainstorming, friends and roommates prioritized this cooperation (i.e., inclusiveness, as introduced by Das [10]) in their final prototypes (Groups C, D, F, K).

Egalitarian governance fell into two different idea categories: group authentication and group approval. Group au-

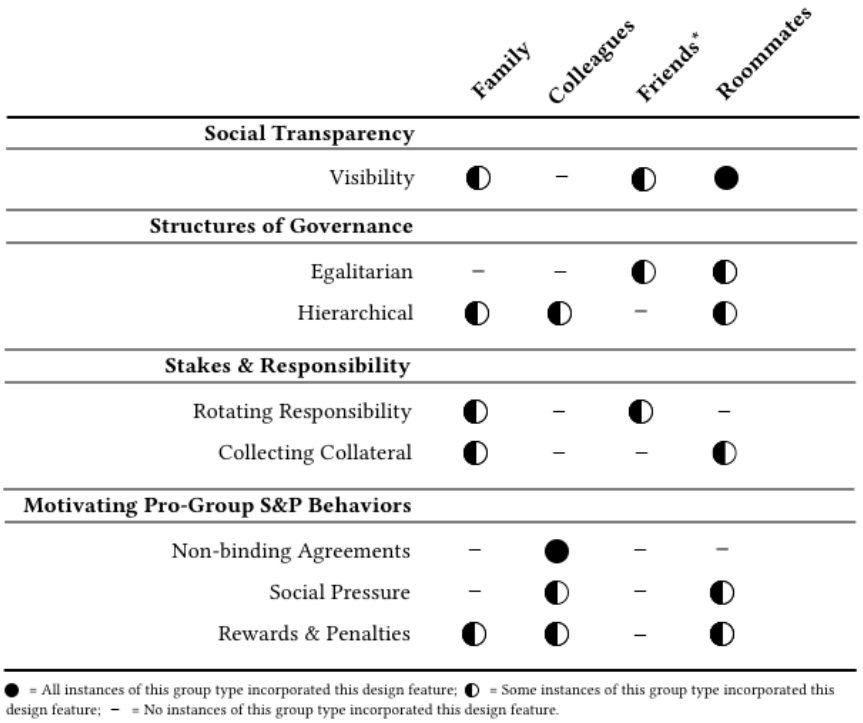


Figure 3: The different design dimensions incorporated into final ideas, organized by group type. * - the friend group type had only two instances across workshops

thentication requires members to approve other members' logging into a resource, akin to two-factor authentication. Group K's final solution Trio used feature: "*It'll send notifications – like a ...a two-factor notification – to all the other members of the group and then at least one of them would have to approve you and say you're in*" (K5). Meanwhile, group approval requires acceptance from multiple members before making changes to or sharing information from the shared resource. For example, when demoing their solution 'Fiing,' Group D noted that members would need unanimous group acceptance using fingerprint identification to make changes to the shared resource."*Nothing can be done without the collective acceptance of everybody who is on that shared account right within the app.*" (D1).

Hierarchical Governance In hierarchical governance, security decisions are made by one or a few members who wield more authority and privilege over the shared resource. There is an implicit assumption that these decision-makers are either more knowledgeable about security and/or technology, more responsible, or are simply the owners of the resource and hence take responsibility over its security.

Unsurprisingly, family scenarios tended to lean on hierarchical governance, where age and technology literacy were more varied. Participants discussed having limited or reduced capabilities for younger and older family members as a way to reduce risk (e.g. using parental controls). Group H (Family) even discussed age-related thresholds for completing purchases: "*So if you have like a teenager, you might want to set it to 10 dollars*" (H4). H4 also noted: "*[An] accountability keeper makes sense for a family. If you let everyone in a family have equal access there is more likely there will be a security breach.*"

Requiring tighter security controls in a family structure might also be attributed to the tendency for families to share more valuable resources with each other. "*If you talk about families that are sharing cars and stuff I'm not just going to let my friends willy-nilly drive my car...especially not my coworkers.*" (J4).

On the flip side, Group B (Roommates) noted that bearing all the responsibility of ownership alone could be inconvenient for the owner. "*What'll make [our idea] easy is one person...approving everything, and it's also the same thing that'll make it hard...since it's that same person that is approving everything and [they] can get kinda annoyed*" (B2).

4.1.3 Stake and Responsibility

The third design consideration for small group S&P controls was the idea that all group members should actively contribute towards the management and upkeep of the group's S&P; in exchange, group members would be permitted to use

Group	Solution	Description
A	Family Communication	Rotate responsibility of who is in charge of password changes. Use shared family Google Drive and physical calendar to track passwords and who is in charge for the month respectively. Passwords share a template that all members are aware of.
B	Roommate Device Password	App to manage access to shared resources. Members receive notification of unrecognized device. Owner of resource can accept or decline. Login history available.
C	Facebook Lockdown	When a Facebook breach occurs on a group members account, friends are notified and auto lockdown activated. Three-step biometric authentication required to re-verify.
D	Fiing	Mobile app through which you can register members sharing a particular resource. App manages authentication into resource. Notifications when members try to make S&P changes, and requires group approval.
E	Sound Entry	Members use voice recognition and location to authenticate into devices. Admin of company adds new members (i.e. colleagues) to the group.
F	Room Me	Mobile app for managing shared resource S&P. RoomMe shows notification of all activity. Security changes and strikes require unanimous approval from all members. Strike system — three strikes = loss of membership.
G	Security Karma	System tracks members' security practices and assigns a security score. Score can be used on an individual or department level. Members can be rewarded (e.g., prizes) or penalized (e.g., affect promotion) based on security score.
H	JKRK Security App	App for managing shared resources. Notifies members of security actions or issues. Members have varying permissions within group. Authorizers for different accounts. Thresholds for spending and permissions and vary per member. Purchases and changes require approval from at least two members.
I	Securiteam	Tracks security practices and assigns a security score. Score can be used on an individual or department level. Scores used for rewards / punishment (e.g., promotion, bonus). Use leaderboard to drive competition to improve security behaviors.
J	Famzees	Family hub for managing resources. Includes chat, activity logging and security alerts for suspicious activity. Only certain members have certain privileges. Parental controls for younger and elder family members.
K	Trio	Group approval required for access into shared resource. Restricted 24 hour access if no one is available to authenticate you.

Table 2: Each group's final prototype design. Workshop 1 - Groups A & B, Workshop 2 - Groups C-E, Workshop 3 - Groups F-H, Workshop 4 - Groups I-K

the resource. The requirement of group-beneficial labor as a condition for access mimics strategies for securing shared resources in the physical world — e.g., makerspaces often trade privileged access to machines in exchange for volunteering time to monitor the makerspace [29] — but is not considered in the design of existing S&P controls. Two strategies emerged to implement this design consideration: (i) periodically rotating responsibilities amongst group members, and (ii) collecting collateral to motivate members.

Rotating Responsibility Generally speaking, users view S&P controls to be secondary concerns in their technology use [18, 53]. As a result, S&P management within a small group context is likely to go completely unnoticed by the larger group, or worse, neglected entirely. Moreover, placing the burden of managing a collectively shared resource on an individual may be considered unfair.

To combat this, participants employed controls to equitably distribute this workload. Group A's solution (Family) 'Family Communication,' leverages a rotational management schedule: "*...We decided we would use basically routine and rotation...so monthly or however they want to schedule, [the password] would be changed by one of the family members but it would be in order. So say it's Mom would do it for this month. Next up is brother and it goes into...a rotation.*"

Equalizing power differentials was another reason to distribute the job. Group K (Friends) discussed rotating the role of administrator such that "*everybody gets to be responsible in the group and, at the same time, only one person doesn't have all the power to make changes without notifying anyone*"

(K2). Erez et al.'s prior work in shared leadership supports this notion, which found that the effects of rotated leadership on self-managed teams were positive, yielding "higher levels of voice and cooperation...appear[ing] to translate into higher levels of team performance" [21].

Collecting Collateral Similarly, groups also thought the use of collateral might improve individual responsibility in upholding S&P standards. By collateral, we are referring to a retainer collected from all group members in exchange for access to the shared resource. Participants reasoned that group members might take S&P more seriously if the stakes were high. For instance, during brainstorming F4 asked whether roommates might "take more initiative" if their own personal information were at stake. This query implies that users recognize the imbalance of effort inherent in some group scenarios.

Collateral appeared to serve as a deposit and as a form of mutual liability. In Group F's solution, subscription payments are automatically deducted from each member's credit card, ensuring that all members are held accountable for making payments. Another group explained why having one's credit card at stake could serve as motivation to increase group S&P: "*I feel like it's linked to your finances; you might be a little more incentivized to respond to an alert like that if it's linked to your credit card account*" (H1).

Group G (Colleagues) also discussed using loosely-defined "sensitive information" as collateral: "*...Everyone has to put in sensitive information. More liability equals increased responsibility, so basically mutually assured destruction if one person kind of leaks the info*" (G1). This parallels prior research on social network systems; users can only control what they share and not what others share [28]. If acting in a negligent manner, the group member not only risks their own security, but also that of the group's. This mutual liability may motivate the group member to comply and act as a cohesive unit.

4.1.4 Promoting Pro-Group S&P Behaviors

The fourth design consideration involves encouraging proactive or preventative S&P behaviors among individual group members for the benefit of the group[4]. While encouraging stronger S&P behaviors is a common consideration in research and practice, our findings provide insight into how groups might formalize this encouragement through design.

Watson et al. found that groups' strategies for securing their shared resources depended on individual members' S&P practices. Further, they found that individual members also had implicit, unspoken agreements to secure their shared resources, but that these implicit agreements often led to frustration and inequity [52]. We found that while designing group S&P controls, many groups considered more explicit mechanisms to motivate each member's S&P behaviors, including: (i) non-binding agreements, (ii) social pressure, and (iii) rewards and penalties.

Non-binding agreements Non-binding agreements are explicitly agreed upon pro-S&P rules, policies and/or best practices each group member agrees to abide by, absent of formal oversight and consequences. Non-binding agreements were common in the colleague's scenario. Group E (Colleagues) discussed having strong corporate policies, appropriate training, and stringent security standards, with E2 noting "*It's the low brow non-tech protocols that really make a difference*" (E2).

Two colleague teams (Groups G & I) from different workshops had similar final ideas around implementing a "security score." Both systems involved assigning a numeric score to individual S&P behaviors and providing personalized feedback for improvement. During their demo, Group G noted that attaching values to security habits can help the individual to self-correct: "*Basically, our idea is analogous to the credit score...if we can put quantifiable numbers...it gives us something to hang our hat on and actionable recommendations and steps to take to beef up our security as a whole, on an individual accountable level*" (G1). Group I also hoped that a personalized security score might motivate the individual to improve on their own: "*Hopefully it's to facilitate better habits...What you're doing is you're trying to instill good habits in that person but he has to learn. It's up to him or her to learn that*" (I2).

Social Pressure Social pressure broadly encompasses the use of competition and social comparison to promote better individual S&P practices. Similar to social transparency, this finding echoes recommendations from prior research [13, 20], but contextualizes it within the context of S&P controls for small, social groups.

Groups used competition as a pressure strategy. Group I (Colleagues), for example, discussed using competition and leaderboards to incentivize individuals, as well as sub-groups within larger groups (e.g., departments within a company), to engage in pro-group S&P behaviors.

Participants from Group F (Roommates) discussed rating each group member in their prototype as a form of social pressure. "*We have a rating system for each and every roommate that is there. So all other roommates rate the person that can be visible on your account page*" (F1). These ratings followed each user from one sharing group to another; the visibility of the ratings and the need to be regarded positively by others served as a way to incentivize users to "act accordingly."

As one participant mentioned, "*For us it was just about using light peer pressure to motivate individual habits*" (I4). Similarly, I1 stated, "*shame works*", echoing prior working by Das et al. [13] who found that pranks and demonstrations were a common trigger for pro-S&P behaviors.

[4] We refer to this as "pro-group"

Rewards and Penalties Using rewards and penalties, groups employed positive and negative reinforcement as a means of influencing individual members' security behaviors.

Both groups G and I talked about rewarding members (i.e., employees) who exhibited pro-S&P behaviours. Group G (Colleagues) noted: "*It's up to the company to decide [how to] incentivize their employees with certain perks, like maybe bonus or like other...gift cards, something like that.*" (G3). Similarly, in Group I's (Colleagues) solution, group members' security scores could be used to reward individual employees or entire departments: "*...And this could be tied to incentives like an Amazon gift card for the department that has the highest security average over the quarter or, you know, maybe a pizza party for that department, something like that*" (I4). Note that only colleague groups leveraged rewards in their final solutions.

Group G and I discussed using the security score to determine penalties. Group G (Colleagues) commented: " *...reversely if they're not scoring so high, you could kick them out of the group, fire them, dock their pay*" (G1). Group J (Family) considered age to be an important element of their design, and talked about revoking privileges for younger members as punishment or as a means of grounding. Group F (Roommates)'s prototype also had a strike feature where members could vote to give a member a strike for improper S&P behavior.

4.2 RQ2. Design Trade-Offs and Challenges

Having distilled a core set of design considerations for social S&P controls, we next explored the perceived trade-offs and challenges of systems that feature these designs from the end-user perspective. Overall, we identified four such challenges: security vs. privacy, herding behavior, security vs. social friction, and coordination costs.

4.2.1 Security vs Privacy

Several ideas to improve group security resulted in the loss of individual members' personal privacy. Participants often discussed how increased social transparency can violate what group members feel comfortable sharing [6, 56], brandishing surveillance in the name of oversight.

We found friend groups preferred to minimize monitoring out of respect for their group members' privacy and independence. "*Since we were friends...we wanted something that wasn't invasive...we're living separately so we're not hanging around each other all the time. Therefore, we don't want to be responsible [for] constantly moderating what other people are doing.* "(K3)

Colleague scenarios were also sensitive about individual member privacy. Group G (Colleagues) were particularly keen to set strict boundaries on what types of activities an employer could monitor, even if these behaviors might pose actual security risks: "*Because we were a business organization..., we drew red lines [around] an employee's internet profile or social media activity. We thought that the red line was companies...infring[ing] on [an employee's] personal time, even though that might have—from a security standpoint — vulnerabilities.*" (G1). Group I (Colleagues) also restricted which scores employees could view, prohibiting a search functionality that could directly reveal the security score of their peers.

On the opposite end of this spectrum, families demonstrated the fewest qualms in monitoring other group members. One participant went so far as to remark that their solution was "*like Big Brother for your family*" (J5).

Overall, we see that although participants value information attained through social transparency, the benefits must be weighed against the infringements to individuals' privacy. Moreover, tolerance of such infringements varies between group types.

4.2.2 Social Herding

The ability to see how other group members have voted or acted in shared governance structures can inhibit the kind of independent thought necessary for group deliberation. This is known as "herd behavior," whereby people make decisions through imitating others' behaviors rather than on the basis of their own opinion. Group H's prototype illustrates how this challenge might stifle deliberation: "*Sarah's device tried to make a 500 dollar purchase at amazon.com and then people can go in and approve or disapprove that transaction...And you can see how many people have already approved it*" (H1).

Previous research in social navigation and end-user S&P suggests that knowing the security decisions of a community of users can help advise those who are unsure in their security and privacy decisions [23]; however, there are a few differences that render this model inadequate for small group security. For one, the size of small groups is often not large enough; it works best when decision behaviors are aggregated over a significant pool of users. Moreover, the decisions being made in small groups are often circumstantial (e.g., Sarah's one-off purchase of 500 dollars) and should be considered on a case-by-case basis, not necessarily by precedent.

4.2.3 Social friction

Groups had to weigh the importance of maintaining social order and a good standing with each other against the requirements of certain security measures.

Group H (Family) discussed the potential friction that could occur if permissions were required from spouses for purchases: "*It would be irritating to have to get authorization from your wife*" (H2). Their resolution was to enforce dollar amount thresholds for purchases: e.g., a $10 purchase may not require approval but a $500 one might. Participants also discussed how penalties could lead to deteriorating relation-

ships. Group F's (Roommates) strike system — used to lock individuals out of group resources if they exhibited poor S&P behaviors — led to a spirited exchange among participants as to how this feature might antagonize group members and negatively impact inter-group relationships.

> H3: *Okay, so suppose it's four roommates you've got and two of the roommates are boyfriend-girlfriend, and then one of them actually did something to deserve the strike. And the other two [roommates] struck down but well, that's my girlfriend, I'm not going to strike her. How do you handle that?*
>
> F4: *In that scenario...if you really believe that that person is a security threat, then you can just cut both of them out. Like, you could just change your guidelines...you can change your subscription rules. Like, just make it so you're only splitting with the one person who wasn't boyfriend-girlfriend...*
>
> G2: *How do you not lose friends?*
>
> H3: *Yeah, I was thinking about that.*
>
> F4: *I mean, the odds of getting a strike — the strike system is more for people who aren't as much like super good friends, because if you're super good friends, odds of you — one being an insider threat... is very slim...*
>
> F2: *We also have the rating system. So the rating system can be like, who we can include as an extra person before you have those strikes involved. So it's like you can put like someone's rating a little bit lower rather than strike them out.*

Here, Group F considered their rating system as an intermediary method to incentivize pro-S&P behaviors and strikes as a last resort. In an ideal scenario, no one would need to get a strike and there would be harmony but, if needed, their strike system was in place to handle serious breaches of shared policy.

These discussions around social friction also led to conversations around what would happen if the social order was to break down. For instance, Group H wondered how members might abuse a strike system by initiating revenge strikes on one another. Group J noted the fragility of the group and it's security very aptly: "*...And if that trust is violated, you know what can happen? If it could be really fragile, someone gets mad at someone and boom everything is...your security is...compromised. So that's a difficult thing to try to mitigate and figure out without making this too difficult for users and over-designing and being too protective*" (J4).

The line between security and social friction must be carefully drawn in order to maintain an effective, social pro-group S&P system.

4.2.4 Coordination Costs

Design considerations like shared governance and stakes and responsibility helped groups more equitably manage their shared resources; however, they also presented coordination costs of time, synchronicity, and social burden.

For example, there may be an unbearable time-delay between requesting for and being granted access to a resource: "*What happens if none of them [group members] are awake or if you're logging in from another part of the world and the timezone doesn't work?*" (K5). In addition, rotating responsibility may introduce additional overhead and coordination. Participants were quick to recognize the inefficiencies that arise as a result of trying to include all members in security decision-making. Resources that require acute, just-in-time access may not be as appropriate using synchronous group authentication.

Another group that utilized group approval and authentication also faced the challenge of not being overly burdensome to other group members: "*'A lot of the ways we were thinking about group security...required multiple people interacting. Which...could be really burdensome sometimes: do I really want my colleague to authenticate every single time I want to see a file?*" (I4).

For colleagues, the answer appeared to be no. But for friends, family and roommates, various concessions were made. Group K's approach issue was to allow for restricted and temporary access to the group member until being authenticated by the group: "*If you're logging into Hulu [without group authentication], it'll somehow disable account settings or it'll disable your account's personal library or something...if they want to watch something on Hulu, they [still] can...but they can't go in and like change the password...There's like a 24-hour grace period so you can stay logged in 24 hours without being authenticated. And then you'll get kicked off after that, and then you won't be able to log back in without getting authenticated.*" (K5) Additionally, Group K also only required one other member to authenticate a login request versus requiring multiple members. They also noted that the fewer members in the group, the more burdensome asynchronous coordination would be.

On the other hand, Group C (Friends) recognized that their tool required extra steps and involvement, but decided that stronger security outweighed any inconvenience. "*For ours because its a Facebook account and maybe like, three-factor verification might seem overboard, but these days, like, everything is so connected, like, people's accounts are connected to other accounts. Your Facebook might be connected to your Whatsapp. Everything is so interconnected. So you can get to any of the other accounts through access into what may seem like the weakest point of entry, so I think it's okay to go overboard...*" (C2)

Overall, many of the social S&P controls participants designed introduced coordination costs. Prior work suggests

users reject security solutions that impose significant time delays [19]. While it is unclear how that result translates to the group context, the challenge remains and must be weighed against the benefits of more social designs.

5 Discussion

To summarize, through a series of participatory design jams, we explored the design space of social S&P controls for shared digital resources (RQ1) along with the trade-offs and challenges therein (RQ2). We consider our core intellectual contribution to be the synthesis of design knowledge entailed by the ideas our participants generated — not the ideas in and of themselves. We also note that while some of our findings mirror and extend prior findings in related disciplines, our work is — to our knowledge — the first to synthesize a design space for social S&P controls for small, social groups.

The social S&P controls that our participants ideated spanned four design dimensions: *social transparency*, or the desire and need for greater visibility into and oversight over individual group members' S&P-relevant behaviors; *structures of governance*, either egalitarian or hierarchical depending on the nature of the group, as a way to facilitate group decision-making on S&P-relevant matters; *stakes and responsibility*, or mechanisms for distributing S&P responsibility among team members proportionate to each member's stake in the shared resource; and, *promoting pro-group S&P behaviors*, or incentives and penalties to encourage pro-group S&P behaviors, such that every member's individual efforts would level up the entire group's security as a whole.However, although we expect the design space we uncovered to capture most shared digital devices and resources, we do not claim that our findings will necessarily apply to all shared digital resources.

With these design considerations came new trade-offs and challenges. Systems that increased social transparency and that explicitly codified rewards and punishment for individual S&P behaviors do so at the expense of individual privacy and by increasing social friction among group members. Systems that required participation from all group members to provide access to a shared resource or to make important S&P relevant decisions (e.g., allowing a new member to join the group) raised concerns of herding behaviors and/or coordination costs. In short, while the design dimensions we have identified provide ample room for design innovation for social S&P controls, we must foreground these trade-offs and challenges in our evaluation of novel social S&P designs.

5.1 Design Implications

5.1.1 Accounting for Group Dynamics

Different group types weighed the social design dimensions we identified differently in their concept designs. Accordingly, it is important to consider group dynamics in the design of novel group S&P controls.

Families preferred hierarchical governance in which one or more authority figures took sole charge of S&P relevant decisions (e.g., parental controls, approval privileges, etc.). Our results show family groups acknowledged the need for simple systems that support a wide variety of technical expertise (novices and experts) and implemented features such as 'parental controls'. Friend groups preferred more leniency in their S&P enforcement measures, opting for non-punitive measures, limited surveillance and monitoring, and unobtrusive access to shared resources. Solutions for friend groups were also generally cooperative and featured egalitarian governance structures. For roommates, increased social transparency was a recurrent feature to curb insider-facilitated outsider threats. Roommates leaned towards egalitarian governance but were generally motivated to protect self-interests. Finally, colleague groups favored evaluative systems with hierarchical governance, in which managers could incentivize employees to encourage individual pro-group S&P behaviors.

To account for these varying preferences, social S&P controls might be designed to be customizable based on group type, or explicitly designed for a specific group type. For example, while parental controls could make sense for some families, a process for collecting collateral may make more sense for roommates with low trust.

5.1.2 Balancing Access and Power

While the results of the design jams primarily speak to designing controls for groups whose threats are outsider threats (insider-facilitated or otherwise) [52], it is also important to consider insider threats from within the group. For example, excess social transparency could be a form of stalkerware for domestic partners in an abusive relationship.

More generally, it is important to actively identify and safeguard against conditions that reinforce imbalances in access and power [9, 56]. For instance, how might members with high levels of technical literacy suppress the agency of those who are less technically savvy? What if all members are not equally informed about the extent of socially transparent activity tracking and have not truly consented for others to view their activity? Should group members who have had shared access for a certain amount of time be granted adverse possession of squatter's rights to those resources? Not all of these scenarios can be addressed purely through design, but designers should account for these scenarios at the onset to help ensure the system does not facilitate undue harm onto users.

5.1.3 Developer Tools to Facilitate Implementation

A steady stream of research has called for the design of more social cybersecurity systems [6, 10, 13, 52]. A key barrier to realizing this vision, however, is the lack of developer tools to

facilitate the implementation and evaluation of such systems. In short, we need usable developer tools that simplifies the prototyping of social S&P controls.

The design dimensions we have uncovered in this work should prove a useful starting point in creating such tools. Existing technologies can be leveraged to implement many of the ideas our participants envisioned. For example, egalitarian governance may be securely realized through Zhang et al.'s PolicyKit system [57] that allows for democratically determined forms of governance in social computing platforms. It may be possible to expand on this system to achieve shared governance over the S&P of shared resources more broadly. Likewise, it should be possible to get the effects of social transparency and community oversight without requiring individuals to reveal private information by using smart contracts on, e.g., the Ethereum blockchain [3]. In such a system, one's activity logs might be kept local but might be checked against previously agreed-upon group policies.

6 Limitations & Future Work

In designing, recruiting for, and conducting our study, we encountered a number of limitations that should be considered to contextualize our findings.

First, while we strove to have a balanced representation between all group types, 21 participants were unable to make the study after being scheduled for a design jam. As a result, the 'Friends' social group had less representation in our design jams than the other three social groups. We had initially intended to run an additional workshop to address this imbalance, but were unable to do so due to restrictions put in place as a result of the COVID-19 pandemic. Nevertheless, the data from the four workshops we did conduct should provide a solid foundation on which future work can build.

Maintaining a representative sample was also difficult in this study. Although we targeted a broad set of people who share digital resources in small social groups, most of our participants were students or young adults. We suspect that people from older age groups likely require greater compensation than what we could provide to attend a two-hour long workshop after work hours, or may have care responsibilities that preclude their participation. Moreover, it is difficult to synchronize the schedules of all workshop participants which could have also posed as a barrier to participation to certain demographic groups.

It's also important to note that many of our participants were not security or design experts — this was an intentional choice on our part, as participatory and co-design processes require end-users who are "experts of their experiences" to cooperate creatively with technical experts [46]. To compensate for their lack of technical knowledge, we played the role of "technical expert" and guided participants through the brainstorming and prototyping process so that they could still productively contribute. Furthermore, participants came into the workshops as strangers. While they were asked to draw from their personal experiences of sharing digital resources with similar groups, designing with strangers likely added a layer of abstraction into participants' ideation. The specific ideas generated were just concepts we used as a design lens to synthesize design implications and are *not* strict recommendations. Nevertheless, our findings provide a useful first step in codifying the design space of for social S&P controls. Future work — perhaps in collaboration with industry partners who can more easily access a broad spectrum of participants — can refine this design space by broadening participant representation. We envision our proposed design space as a catalyst for future innovation and a guide for implementing and evaluating novel social S&P controls for shared digital resources.

7 Conclusion

Through a codification of ideas produced in participatory design jams, we found that there are four key design dimensions to consider in designing social S&P controls for shared digital resources: (i) that social transparency is important to all group types and a means of maintaining a sense of control over a collectively owned and shared digital resource; (ii) that groups enact either an egalitarian or hierarchical structure of governance to collectively manage their S&P; (iii) that groups want ways for all members to be invested in the S&P of the group and use collateral or rotating responsibility to equalize stake; and, (iv) that groups want to implement mechanisms to promote positive S&P behaviors in individual members, thus improving security for the group as a whole.

In considering these design dimensions to brainstorm novel small group S&P controls, we also identified trade-offs that were made and new challenges that arose: balancing individual privacy with group need for transparency; mitigating social herding tendencies; diminishing social friction that may occur through making explicit the group's S&P rules and policies; and, managing costs that arose from asynchronous coordination. Lastly, we reflected on participants ideas and how group type influences the relative weight of the aforementioned design dimensions, argued for the need to get ahead of potential problems with access and power, and discussed the feasibility of implementing these ideas using existing technologies. In short, our work provides a strong foundation for future innovation in building end-user S&P controls for digital resources shared among small, social groups.

Acknowledgments

This work was generously funded, in part, by NSF SaTC grant #1755625. We would also like to thank the members of the GT SPUD Lab for providing instructive feedback throughout the duration of the work.

References

[1] Mark S. Ackerman. The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility. *Human–Computer Interaction*, 15(2-3):179–203, sep 2000.

[2] A. Tece Bayrak. Jamming as a design approach. Power of jamming for creative iteration. *The Design Journal*, 20(sup1):S3945–S3953, jul 2017.

[3] Andreas Bogner, Mathieu Chanson, and Arne Meeuw. A Decentralised Sharing App running a Smart Contract on the Ethereum Blockchain. In *Proceedings of the 6th International Conference on the Internet of Things - IoT'16*, volume 07-09-Nove, pages 177–178, New York, New York, USA, 2016. ACM Press.

[4] Eva Brandt, Thomas Binder, and Elizabeth Sanders. Tools and techniques: Ways to engage telling, making and enacting. In Jesper Simonsen and Toni Robertson, editors, *Routledge International Handbook of Participatory Design*, chapter 7, pages 145–181. Routledge, oct 2012.

[5] A. J. Bernheim Brush and Kori M. Inkpen. Yours, Mine and Ours? Sharing and Use of Technology in Domestic Environments. In John Krumm, Gregory D Abowd, Aruna Seneviratne, and Thomas Strang, editors, *UbiComp 2007: Ubiquitous Computing*, pages 109–126. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.

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

[7] Juliet Corbin and Anselm Strauss. *Basics of Qualitative Research (3rd ed.): Techniques and Procedures for Developing Grounded Theory*. SAGE Publications, Inc., 2455 Teller Road, Thousand Oaks California 91320 United States, 3rd edition, apr 2008.

[8] Jonathan Courtney. Lightning Design Jams: the exercise that will solve all of your problems | Inside Design Blog, 2018.

[9] Alexei Czeskis, Ivayla Dermendjieva, Hussein Yapit, Alan Borning, Batya Friedman, Brian Gill, and Tadayoshi Kohno. Parenting from the pocket: Value tensions and technical directions for secure and private parent-teen mobile safety. *ACM International Conference Proceeding Series*, 2010.

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

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

[12] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. The Effect of Social Influence on Security Sensitivity. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014*, pages 143–157. USENIX Association, 2014.

[13] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. Increasing Security Sensitivity With Social Proof. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS '14*, pages 739–749, New York, New York, USA, 2014. ACM Press.

[14] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 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*, pages 1416–1426, New York, New York, USA, 2015. ACM Press.

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

[16] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I. Hong. 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*, pages 1–12, New York, New York, USA, 2018. ACM Press.

[17] Paul DiGioia and Paul Dourish. Social navigation as a model for usable security. In *Proceedings of the 2005 Symposium on Usable Privacy and Security*, SOUPS '05, page 101–108, New York, NY, USA, 2005. Association for Computing Machinery.

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

[19] Serge Egelman, A.J. Bernheim Brush, and Kori M. Inkpen. Family accounts. In *Proceedings of the ACM*

2008 conference on Computer supported cooperative work - CSCW '08, page 669, New York, New York, USA, 2008. ACM Press.

[20] Serge Egelman, Andreas Sotirakopoulos, Ildar Muslukhov, Konstantin Beznosov, and Cormac Herley. Does my password go up to eleven? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13*, page 2379, New York, New York, USA, 2013. ACM Press.

[21] Amir Erez, Jeffrey A. Lepine, and Heather Elms. Effects Of Rotated Leadership and Peer Evaluation on the Functioning and Effectiveness of Self-Managed Teams: A Quasi-Experiment. *Personnel Psychology*, 55(4):929–948, dec 2002.

[22] Thomas Erickson and Wendy A. Kellogg. Social translucence. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 7(1):59–83, mar 2000.

[23] Jeremy Goecks, W. Keith Edwards, and Elizabeth D. Mynatt. Challenges in supporting end-user privacy and security management with social navigation. In *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*, page 1, New York, New York, USA, 2009. ACM Press.

[24] Maia Jacobs, Henriette Cramer, and Louise Barkhuus. Caring About Sharing. In *Proceedings of the 19th International Conference on Supporting Group Work - GROUP '16*, pages 235–243, New York, New York, USA, 2016. ACM Press.

[25] Katie Jones. How to Run a Design Jam - UCIMHCID - Medium, 2017.

[26] Joseph 'Jofish' Kaye. Self-reported password sharing strategies. In *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11*, page 2619, New York, New York, USA, 2011. ACM Press.

[27] Seckyoung Loretta Kim and Seokhwa Yun. The effect of coworker knowledge sharing on performance and its boundary conditions: An interactional perspective. *Journal of Applied Psychology*, 100(2):575–582, 2015.

[28] Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. We're in it together: Interpersonal management of disclosure in social network services. In *Conference on Human Factors in Computing Systems - Proceedings*, pages 3217–3226, New York, New York, USA, 2011. ACM Press.

[29] Jacob Logas, Ruican Zhong, Stephanie Almeida, and Sauvik Das. Tensions between access and control in makerspaces. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW3):1–33, 2021.

[30] Andrés Lucero and Tuuli Mattelmäki. Good to see you again. In *Proceedings of the 2011 Conference on Designing Pleasurable Products and Interfaces - DPPI '11*, page 1, New York, New York, USA, 2011. ACM Press.

[31] Brady Mason. Innovation Jam: A Creative Workshop | International blog.

[32] Michael Mateas, Tony Salvador, Jean Scholtz, and Doug Sorensen. Engineering ethnography in the home. In *Conference companion on Human factors in computing systems common ground - CHI '96*, pages 283–284, New York, New York, USA, 1996. ACM Press.

[33] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. "She'll just grab any device that's closer". In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 5921–5932, New York, NY, USA, may 2016. ACM.

[34] Michelle L. Mazurek, Brandon Salmon, Richard Shay, Kami Vaniea, Lujo Bauer, Lorrie Faith Cranor, Gregory R. Ganger, Michael K. Reiter, J. P. Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, and Jenny Olsen. Access control for home data sharing. In *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*, page 645, New York, New York, USA, 2010. ACM Press.

[35] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), November 2019.

[36] Jacqueline McIntosh and Bruno Marques. Designing for culturally-diverse communities. The role of collaborative, interdisciplinary design-led research. *The Journal of Public Space*, 2(3):21, dec 2017.

[37] Bulent Menguc, Seigyoung Auh, and Young Chan Kim. Salespeople's Knowledge-Sharing Behaviors with Coworkers Outside the Sales Unit. *Journal of Personal Selling & Sales Management*, 31(2):103–122, mar 2011.

[38] Darakhshan J. Mir, Yan Shvartzshnaider, and Mark Latonero. It Takes a Village: A Community Based Participatory Framework for Privacy Design. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 112–115. IEEE, apr 2018.

[39] Michael Nebeling and Katy Madier. 360proto: Making Interactive Virtual Reality & Augmented Reality Prototypes from Paper. In *Proceedings of the 2019 CHI*

Conference on Human Factors in Computing Systems - CHI '19, pages 1–13, New York, New York, USA, may 2019. ACM Press.

[40] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, and Laura Dabbish. Share and Share Alike? An Exploration of Secure Behaviors in Romantic Relationships. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2018.

[41] Samuli Pekkola, Niina Kaarilahti, and Pasi Pohjola. Towards formalised end-user participation in information systems development process. In *Proceedings of the ninth conference on Participatory design Expanding boundaries in design - PDC '06*, volume 1, page 21, New York, New York, USA, 2006. ACM Press.

[42] Daniela K. Rosner, Saba Kawas, Wenqi Li, Nicole Tilly, and Yi-Chen Sung. Out of time, out of place: Reflections on design workshops as a research method. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, CSCW '16, page 1131–1141, New York, NY, USA, 2016. Association for Computing Machinery.

[43] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. Password sharing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '07*, pages 895–904, New York, New York, USA, 2007. ACM Press.

[44] Manya Sleeper, Rebecca Balebako, Sauvik Das, Amber Lynn McConahy, Jason Wiese, and Lorrie Faith Cranor. The post that wasn't. In *Proceedings of the 2013 conference on Computer supported cooperative work - CSCW '13*, page 793, New York, New York, USA, 2013. ACM Press.

[45] Stephen Snow, Dorota Filipczuk, Stephen Viller, and Richard Gomer. Design Jam as a Pedagogy. In *Proceedings of the 31st Australian Conference on Human-Computer-Interaction*, pages 128–137, New York, NY, USA, dec 2019. ACM.

[46] Marc Steen, Menno Manschot, and Nicole De Koning. Benefits of co-design in service design projects. *International Journal of Design*, 5(2), 2011.

[47] Erik Stolterman and Mikael Wiberg. Concept-Driven Interaction Design Research. *Human–Computer Interaction*, 25(2):95–118, may 2010.

[48] H. Colleen Stuart, Laura Dabbish, Sara Kiesler, Peter Kinnaird, and Ruogu Kang. Social transparency in networked information exchange. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work - CSCW '12*, page 451, New York, New York, USA, 2012. ACM Press.

[49] Michael Toomim, Xianhang Zhang, James Fogarty, and James A. Landay. Access control by testing for shared knowledge. In *Proceeding of the twenty-sixth annual CHI conference on Human factors in computing systems - CHI '08*, page 193, New York, New York, USA, 2008. ACM Press.

[50] Kirsikka Vaajakallio and Tuuli Mattelmäki. Collaborative design exploration. In *Proceedings of the 2007 conference on Designing pleasurable products and interfaces - DPPI '07*, number August, page 223, New York, New York, USA, 2007. ACM Press.

[51] Valentina Vezzani and Tang Tang. Investigating the Potential of Design Jams to Enhance Sustainable Design Education. In *NordDesign 2014 Conference, NordDesign 2014*, pages 037–046. Aalto Design Factory, Aalto University, 2014.

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

[53] Alma Whitten and J. D. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. *8th USENIX Security Symposium*, 1999.

[54] Monica Whitty, James Doodson, Sadie Creese, and Duncan Hodges. Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychology, Behavior, and Social Networking*, 18(1):3–7, jan 2015.

[55] Qian Yang, Jina Suh, Nan Chen Chen, and Gonzalo Ramos. Grounding interactive machine learning tool design in how non-experts actually build models. In *DIS 2018 - Proceedings of the 2018 Designing Interactive Systems Conference*, pages 573–584, New York, NY, USA, jun 2018. Association for Computing Machinery, Inc.

[56] Eric Zeng and Franziska Roesner. Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study. *Proceedings of the 28th USENIX Security Symposium*, pages 159–176, 2019.

[57] Amy X Zhang, Grant Hugh, and Michael S Bernstein. PolicyKit: Building Governance in Online Communities. 2020.

[58] John Zimmerman, Jodi Forlizzi, and Shelley Evenson. Research through design as a method for interaction design research in HCI. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 493–502, 2007.

A Design Jam Materials and Surveys

A.1 Screener Survey

1. Are you 18+?
2. Do you share digital devices (e.g. Computer, phone, Xbox, Amazon Echo etc.) or digital accounts (e.g. Netflix, Bank account, Instagram, GroupMe, Google Drive etc.) with any of the below social groups? Select all that apply.
3. Are you a designer or developer?
4. Are you available to participate in this study on any of the following workshop dates?
5. Name?
6. Email?
7. Phone Number?

A.2 Workshop Exit Survey

1. Which group's solution is most relevant to your personal experience?
2. Why is <insert solution selected> solution relevant to your personal experience?
3. Please describe a scenario you would use <insert solution selected>?
4. Optional demographic questions (Age, Gender identity, Ethnicity, Education Level, Employment Status)

A.3 Workshop Discussion Questions

1. What S&P principle does your idea fall under? Why?
2. How did your specific group scenario/dynamics impact your design decisions?
3. Consider the different resources your group shares. Does your idea help with all, one, or some of the resources– why?
4. Did you determine security needs based on the type of resource? If yes, how?
5. What might make your system easy or hard to use? (limitations?)
6. As a <user/designer/developer> what was easy about brainstorming and designing a group security solution?
7. As a <user/designer/developer> what was difficult about brainstorming and designing a group security solution?

A.4 S&P Cheat Sheet for Participants

A.4.1 Security & Privacy

1. Security: Refers to how your personal information is protected.
2. Privacy: Relates to any rights you have to control your personal information and how it's used.

A.4.2 Group Cybersecurity Principles

1. Observability: Making it easy for people to observe and emulate good security behaviors. *Example: Someone observes their friend using a password manager, then decides to use one as well.*
2. Cooperation: Allowing people to act together for mutual security benefits. *Example: Users of a website can leave "notes" for future users about the safety and security of that site OR People collaborating to condense lengthy and dense terms of service into quick, easy-to-read bullet points.*
3. Stewardship: Allowing people to act on behalf of others' cybersecurity benefits. *Example: Helping a friend set up their wireless router.*

A.4.3 Group Threat Opportunities

1. Insider Threats: Threats from within the group. *Example: Someone screenshotting a private image sent to the group.*
2. Outsider Threats: Threats from outside of the group. *Example: A stranger uses your laptop that you've left open.*
3. Insider-facilitated Outsider Threats: Threats from outside that are made possible by the actions of insiders. *Example: A member of a group shares the account password with someone outside the group.*

B Participant Demographics

ID	Age	Gender	Race	Education	Employment	ID	Age	Gender	Race	Education	Employment
A1	25-34	M	B	M.S.	FT	G1	35-44	M	A	PD	FT
A2	35-44	F	NA	M.S.	U	G2*	25-34	M	H	B.S.	S
A3	25-34	F	B	M.S.	FT	G3*	18-24	F	A	SC	FT
A4	18-24	M	O	B.S.	U	G4*	25-34	F	W	M.S.	S
B1	18-24	F	A	B.S.	S	H1	18-24	F	A	S.C.	S
B2	25-34	M	B	SC	FT	H2	25-34	F	W	B.S.	FT
B3	18-24	M	A	M.S.	S	H3	45-54	M	B	PhD	FT
B4	25-34	F	W	M.S.	S	H4*	25-34	M	W	B.S.	S
C1	25-34	M	B	SC	FT	I1*	25-34	M	A	B.S.	S
C2	25-34	F	B	M.S.	FT	I2*	18-24	F	A	SC	S
C3	25-34	F	B	B.S.	FT	I3*	18-24	F	W	SC	S
D1	25-34	F	W	B.S.	FT	I4	35-44	M	W	M.S.	FT
D2*	35-44	M	B	SC	FT	J1	35-44	F	A	M.S.	S
D3	25-34	M	NA	SC	S	J2	18-24	F	W	SC	S
E1	18-24	F	A	SC	S	J3	25-34	M	W	SC	FT
E2*	35-44	M	W	PD	FT	J4	35-44	M	W	SC	FT
E3	25-34	M	A	M.S.	S	J5	35-44	M	B	M.S.	FT
F1	18-24	M	A	B.S.	S	K1	18-24	M	NA	M.S.	S
F2*	18-24	F	A	SC	S	K2	25-34	M	A	PhD	S
F3*	18-24	M	A	HS	S	K3	25-34	M	W	M.S.	S
F4	18-24	M	A	HS	S	K4	18-24	M	A	SC	S
						K5	18-24	M	A	SC	S

Table 3: Participant Demographics. Columns include Participant ID, Age, Gender, Race, Education and Employment. Race abbreviations: (Black, White, Asian, Hispanic or Latino, Other and N/A i.e declined to state). Education abbreviations: (High School Graduate, Some College, Bachelors , Masters , Professional and Doctoral). Employment abbreviations: (Full Time, Student, Unemployed). * - participant assigned to a group type they did not share resources with (per their screener survey answers)