Tensions between Access and Control in Makerspaces

JACOB LOGAS and RUICAN ZHONG*, Georgia Institute of Technology
STEPHANIE ALMEIDA, Georgia Institute of Technology
SAUVIK DAS, Georgia Institute of Technology

Makerspaces have complex access control requirements and are increasingly protected through digital access control mechanisms (e.g., keycards, transponders). However, it remains unclear how space administrators craft access control policies, how existing technical infrastructures support and fall short of access needs, and how these access control policies impact end-users in a makerspace. We bridge this gap through a mixed-methods, multi-stakeholder study. Specifically, we conducted 16 semi-structured interviews with makerspace administrators across the U.S. along with a survey of 48 makerspace end-users. We found four factors influenced administrators' construction of access control policies: balancing safety versus access; logistics; prior experience; and, the politics of funding. Moreover, administrators often made situational exceptions to their policies: e.g., during demand spikes, to maintain a good relationship with their staff, and if they trusted the user(s) requesting an exception. Conversely, users expressed frustration with the static nature of access control policies, wishing for negotiability and for social nuance to be factored into access decisions. The upshot is that existing mechanisms for access control in makerspaces are often inappropriately static and socially unaware.

CCS Concepts: • **Security and privacy** → **Social aspects of security and privacy**; **Usability in security and privacy**; • **Human-centered computing** → *Collaborative and social computing design and evaluation methods.*

Additional Key Words and Phrases: social cybersecurity, participatory design, usable security, groups, cscw

1 INTRODUCTION

Access control is a critical component of ensuring the security of protected, shared physical spaces and the resources within those spaces. Increasingly, these shared physical spaces are secured with digital access control mechanisms. Yet, despite evidence suggesting context-dependent, nuanced access preferences among end-users and administrators [15], most spaces default to a binary access dichotomy, relying on mainly on card-based systems (71%) [3].

Prior work suggests existing digital access control mechanisms for shared spaces map poorly onto real-world access needs [2]. Yet, little is known about where the breakdown lies between what end-users and administrators desire in access control for shared spaces and how existing systems might contribute to and exacerbate those breakdowns. Building on this prior work, we conducted a mixed-methods investigation into the dual perspectives of space administrators and end-users with respect to access control in the context of makerspaces.

*Both authors contributed equally to this research.

Authors' addresses: Jacob Logas, logasja@gatech.edu; Ruican Zhong, rzhong34@gatech.edu, Georgia Institute of Technology, Atlanta, Georgia; Stephanie Almeida, salmeida6@gatech.edu, Georgia Institute of Technology, Atlanta, Georgia; Sauvik Das, das@gatech.edu, Georgia Institute of Technology, Atlanta, Georgia.

0004-5411/2020/8-ART111 $15.00
https://doi.org/10.1145/1122445.1122456

Makerspaces present an interesting opportunity to explore digital access control strategies and breakdowns for shared spaces. They incorporate a broad set of constraints: many rely on a patchwork of administrators like permanent staff, part-time staff and volunteers, complicating coordination and enforcement of access control policies; they are often underfunded and have limited resources to expend on secondary concerns like access control; they contain machinery which may require individualized access control policies contingent on training and other safety precautions (e.g., the presence of a chaperone); and, they have a diverse and dynamically changing set of daily users whose access needs are constantly evolving and difficult to predict [7, 8, 14, 21].

We performed semi-structured interviews with 16 makerspace administrators across the United States and conducted an online survey with 48 makerspace users between March and May of 2020. Our goal was to explore breakdowns in how and why digital access control policies were created, enforced, and navigated, contrasting the perspectives of administrators and end-users, and highlighting opportunities for design. Specifically, we aimed to address the following three research questions:

RQ1: What factors influence access control policies in makerspaces?
RQ2: Why and under what circumstances do administrators make exceptions to access control policies in makerspaces?
RQ3: How do access control policies frustrate and encumber end-users in accessing a makerspace and its machines?

We found four factors weighed into administrators' construction of access control policies: (i) safety, or granting access contingent on context-specific safety criteria (e.g., the presence of a chaperone, training certification); (ii) logistics, including capacity and the synchronicity between staff and end-user schedules; (iii) experience, or prior exposure to creating and refining access control policies; and, (iv) funding, which sometimes required granting privileged access or selective restrictions to certain groups of users. Administrators also made situational exceptions to the policies they created: e.g., they would extend operational hours during demand spikes and they would afford staff members and users they trusted some leeway. End-users, however, expressed frustration with the static and binary nature of access control policies in makerspaces and desired socially and contextually aware access control.

Concretely, we contribute:

- the first multi-stakeholder study on digital access control breakdowns in shared makerspaces;
- a descriptive model for how makerspace administrators craft, refine and make exceptions to access control policies; and,
- a set of prescriptive design recommendations for digital access control systems in shared physical spaces.

2 BACKGROUND AND RELATED WORK

2.1 Access Control

Access control is the mechanism through which permissions to a resource — either physical or digital — are granted or denied. Usable access control has been extensively studied in prior work, primarily outside of the context of makerspaces.

Prior work shows existing systems to set and enforce access control policies often fail to meet user needs. Mazurek et al. examined access control of data and accounts on shared devices in the home [15]. Their interviews revealed that users often construct ad-hoc access control mechanisms as their ideal access control policies are more complex than allowed by existing systems. Users found a-priori policy specifications to be insufficient and users' mental models of access control were misaligned with actual system designs. Bauer et al. evaluated a physical space access control

system to model ideal access control policies in situ [2]. They found that, in contrast to a key system, a system that allows for delegation — i.e., the temporary transfer of access rights — better matches users' optimal access policy.

Prior work also highlights that existing access control systems are often ambiguous, which can cause policy conflicts that are difficult to resolve and can result in unintended access [19]. Egelman et al. investigated the ambiguity of and a solution to Facebook's audience selection mechanism as well as the usefulness users get from the controls [6]. Participants were presented with the standard access controls or a Venn diagram showing the communities with access to a post. They were then asked to choose access for a set of posting scenarios with both tools. The Venn diagram accounted for a higher incidence of participants correctly configuring access options, low information leak. Though, in the followup interview participants admitted they rarely change the privacy settings from default, apathetic about the potential leak. Ringer et al. developed novel user-driven access control in Operating Systems (OS) to provide a method for fine-grained access to system resources (e.g. microphone) [20]. In this work, the investigators developed a method for explicit consent from users for use of sensitive permissions on Android OS.

We build on and extend knowledge of optimal access control policies for end-users in a novel use-context: the makerspace. As we will detail in the next section, makerspaces present a broad set of constraints that complicate the setting and enforcement of access control policies.

2.2 Understanding Makerspaces

Makerspaces present a unique challenge for physical access control: the tools embedded within them are expensive and can cause significant harm if used improperly, requiring stringent access control policies; yet, the culture of makerspaces promotes open exploration and "learning through making" [17]. To improve access control for makerspaces, thus, it is important to understand their underlying culture. Prior research has sought to understand the maker movement's culture as well as how to improve makerspace accessibility with usage metrics and analysis.

2.2.1 Culture. Since the "maker revolution" [25] started in 2009, researchers have studied maker culture and how it manifests in makerspaces; a place for exploration, community, functionality, and openness [24]. Han et al. found technical, economic, and social support were major factors of makerspace accessibility. Technical training programs helped users gain autonomy and competence, while social support determined community openness [9]. Even with an overall maker culture, individual makerspace case studies reveal cultures that blend local community and maker culture [7, 11, 14, 16, 21]. Building on this prior work, we investigate the degree to which culture influences makerspace policy.

Prior work also investigated who administers makerspaces and how their values influence staffing preferences. Koh et al. interviewed administrators at makerspaces to identify administrator core competencies finding makerspace administrators: learn quickly, adapt, collaborate, advocate, and serve a diverse user-base [12]. Gottbrath et al. studied how staff sufficiency was related to the size of a makerspace and how staff recruitment balanced accessibility and safety [8]. Similarly, Radniecki et al. found administrators prefer hiring students with niche expertise to better contribute to the learning environment [18]. Davies et al. conducted a case study at a student-run makerspace, finding trust was the key to management particularly when reforming policies [5]. Here, we further develop an understanding of administrator values and how it effects policy.

2.2.2 Use. Administrators create access policies based on the information they have; prior work investigated the scope of data available, what the data can reveal about use, and methods for exposing greater information. Imam et al. investigated the depth of existing user tracking metrics [10] and Schoop et al. analyzed the data to find trends [22]. Wildbolz et al., Darwin et al., and Licks

et al. proposed tools integrating automatic sign-in with the lab and its equipment for more granular user metrics [4, 13, 23], with the thought that this would aid administrators in optimizing use. We build upon this work by investigating if and how administrators use the data available to them for their duties.

3 METHODOLOGY

Recall our three key research questions are what factors influence access control policies in makerspaces, why and under what circumstances do administrators make exceptions to access control policies in makerspaces, and how do access control policies frustrate and encumber end-users in accessing a makerspace and its machines. To address these questions, we ran a mixed-methods investigation consisting of two studies: semi-structured interviews and a survey with end-users. To answer the first and second research questions, we conducted semi-structured interviews with makerspace administrators from all over the United States to unpack access control motivations, methods for handling exceptional circumstances, and where existing processes and structures fall short. To answer the third research question, we conducted a survey with end-users to understand how they navigate existing access control policies and their frustrations thereof. Our methodology was approved by an IRB.

3.1 Semi-structured interviews with administrators

Our interviews with space administrators focused on four broad categories of questions: the roles and responsibilities of the administrator within their makerspace with respect to generating and enforcing access control policies; the busyness of the makerspace and its bearing on access control; the access control policies of the makerspace, itself, as well as the machines within the makerspace; and, the technical methods and systems used to enforce access control policies.

3.1.1 Procedure. Due to COVID-19, the interviews were virtually held over Zoom, and lasted approximately forty minutes. The administrators signed the consent document and were asked to provide demographic data. Once completed, we asked the administrators questions about the space. First, we asked about their roles and responsibilities. We asked them about their primary job function, the main purpose of the space, what responsibilities they held, what they spent the most time on, and what was the easiest and most difficult part of their jobs. Second, we asked about how busy the space was (e.g., how many people visit the space daily, paid staff or volunteers, number of staff per shift). Third, we asked how policies were created such as *How do you define your policies?* and *How do you enforce your policies?*. Finally, the last set of questions was about how access control policies affected the security of the space. We asked questions such as *What do you do to ensure safe usage of machinery* and *How do people gain access to the space.*

3.1.2 Recruitment & Compensation. In creating a list of potential participants, we used a combination of snowball sampling and cold-emails. We began recruiting individuals in local makerspaces for pilot interviews. These administrators then referred us to other connections. Additionally, we searched online for makerspaces associated with major universities in the United States. After reaching out to them, we began reaching out to smaller makerspaces including those in community colleges, nonprofit-based makerspaces, and for-profit-based makerspaces. In total, we reached out to 146 makerspaces, 16 of whom responded and completed our interviews. The interview participants were not compensated.

3.1.3 Analysis. We employed thematic analysis on the interviews. Each interview was recorded and transcribed using the OtterAI tool [1]. Two researchers extracted excerpts relevant to the research questions and independently coded each excerpt. These two researchers came together

to discuss their independent codes until settling on a final codebook. The final codebook had 12 codes, including themes like *individual judgement*, *trust in end-users*, *capacity*, *synchronizing staff and user schedules*, *staff sufficiency*, *experience*, and *keeping up with demand*. A third researcher then joined and helped code the remaining excerpts with the final codebook.

After coding the remaining excerpts, we calculated descriptive statistics based on the codes and common themes we discovered. We then grouped the themes focusing on access control and admin role to answer the first research question. We also grouped the themes focusing on how administrators enforce policies to answer the second research question.

3.2 Surveys with end-users

To answer RQ3, we complemented our administrator interviews with an end-user survey. The purpose of the survey was to understand how makerspace access control policies affected end-user interactions with the space and the likelihood of certain access control situations occurring. The survey questionnaire consisted of seven sections: information about the makerspace; busyness; access authentication; special training for machine usage; chaperones for machine usage; permissions protocol; and, the likelihood of specific scenarios occurring. The survey consisted of 59 questions and took participants about 8.5 minutes to complete. We provide the full survey questionnaire in the supplementary materials for review.

3.2.1 Procedure. To participate in the study, the users filled out a Qualtrics survey and went from section to section answering questions about their experience, and answered how likely certain situations were to occur in the spaces.

3.2.2 Recruitment & Compensation. In total, 48 participants completed the survey. We approached makerspace-specific and general technology-focused groups on social media. Participants were entered into a raffle of 10 people to win a $25 gift card.

3.2.3 Analysis. After participants filled out the survey, we looked at the results in the Reports section of Qualtrics. This section automatically organized the results from the survey into various charts which allowed us to easily analyze the data to see where the trends were. These graphs were based on the multiple choice questions we asked the users. We performed open coding for the free response questions asked in the survey using thematic analysis using a method similar to the interview results. Two researchers extracted excerpts related to our third research question from the free response questions. The excerpts were then analyzed for themes and codes to develop the final code-book.

After coding the remaining free response questions, we focused on questions relating to access control of the space, *How do you usually access the makerspace?*, *Are you able to access a makerspace without trouble using the current authentication method?* with a followup question of *Please briefly describe how the current authentication method has caused any trouble, and if possible, some suggestions to improve the current method.*, *Generally, how late are the makerspaces open?*. We also looked at responses regarding access control to machines, specifically asking *Have you ever felt the special training is repetitive or unnecessary* with a followup question of *Please briefly describe why you felt the special training is repetitive or unnecessary, and if possible, give some suggestions.* and *Do the machines you want to access typically have a long queue?*. We then cross-referenced questions to see if responses were dependent on the type of space. For example, we checked to see if there was anything in common between spaces open 24/7 versus spaces open only until the evening.

	Gender	Full-Time	Population	Size	For Profit
P1	Female	✗	College Students & Faculty	Medium	✓
P2	Male	✗	College Students & Faculty	Large	✗
P3	Male	✗	College Students	Small	✗
P4	Male	✓	College Students	Large	✗
P5	Male	✓	College Students	Medium	✗
P6	Male	✓	College Students & Faculty	Large	✗
P7	Male	✗	College Students, K12 Students	Large	✗
P8	Female	✓	College Students	Small	✗
P9	Male	✓	College Students	Medium	✗
P10	Male	✓	College Students, Community	Small	✗
P11	Male	✗	College Students	Large	✗
P12	Male	✓	Community	Medium	✓
P13	Female	✓	Community	Small	✓
P14	Male	✗	Community	Medium	✗
P15	Female	✗	Community	Small	✓
P16	Male	✓	Community	Large	✓

Table 1. Administrator demographics. (The small makerspaces had 15-20 users per day; medium makerspaces had 30-40 users per day; large makerspaces had 40-100 users per day)

4 DATASET

4.1 Interview data

We conducted the semi-structured interview with 16 makerspace administrators where 9 identified administration as their primary responsibility. University owned makerspaces were the majority of the respondents (11) with others either privately owned or publicly run. Table 1 summarizes the demographics of the interviewees and makerspaces.

4.2 Survey data

We received 52 responses from the survey, and 48 of them completed the entire survey. Of the 48 participants, 14 identified as male and 24 were full-time students (Table 2).

Female	68.75%
Male	29.17%
Other	2.08%

(a) Gender

18-24	50%
25-34	31.25%
35-44	14.58%
45-54	4.17%

(b) Age

Student	50%
Employed Full-time	31.25%
Employed Part-time	10.42%
Self-Employed	4.17%
Unemployed	4.17%

(c) Employment Status

Table 2. Demographics of online survey participants

5 RESULTS

Our first two research questions pertain to how and why makerspace administrators create access control policies, how they enforce these policies, and how they navigate making case-by-case exceptions. We address these questions by analyzing the administrator interview transcripts. Our third and final research question pertains to the impact of access control policies on end-user

experience within the makerspace. We address this question by analyzing the end-user survey responses. Note that we considered both access control to the makerspace itself, as well as to the individual machines in the space.

5.1 RQ1: Factors that Influenced Access Control Policies

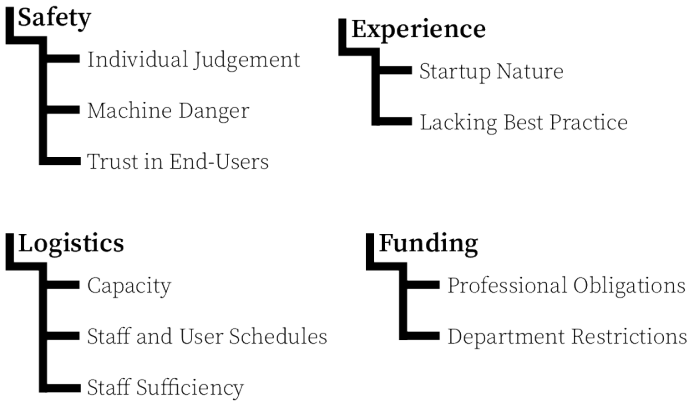

Fig. 1. Factors that influenced Access Control Policies

We found that four factors weighed into decisions to create and enforce access control policies in makerspaces Fig. 1, each of which posed complex challenges that could not be addressed by existing strategies: safety, logistics, administrator experience with best practices for access control, and the source of funding.

5.1.1 Safety. The first factor that influenced how administrators created access control policies for their makerspaces was safety: specifically, how they balanced safety versus access, which were sometimes at odds [7]. P4 highlighted this tension:

"With a space like this, there's . . . the constant battle between making your space as accessible and useful as possible, while still making sure that it stays safe and. . . regulated and can continue being maintained long term. [G]iven how much those two are at odds, often, that's quite difficult." (P4)

Three sub-factors influenced how administrators incorporated considerations of safety into their access control policies: individual judgment, the inherent danger of the machines in the space, and trust in end-users.

Individual judgement. P6 subsumed the tension between access and safety, among other things, under the more abstract heading of "culture", indicating that balancing these two competing considerations is a matter of individual judgment:

"The most important thing is safety . . . , but I put culture in front of that because it includes safety, but it also includes other things like how you operate in the space, how you serve the community . . . " (P6)

Later in the interview, P6 revealed that they experimented with keeping the space open later during busy periods, suggesting that despite safety being "the most important" consideration, they were willing to make concessions to afford greater access in some circumstances:

"[W]e had some late evening hours access that . . . we provided to our students staff in December." (P6)

Machine danger. The second point of safety that influenced access control policy creation is the danger of the machines in the space. Makerspaces have machines that can be dangerous if operated incorrectly, so unfettered access can result in safety concerns. In contrast, cautious access control policies can hinder end-users ability to make. Generally, makerspaces with less dangerous equipment had looser access control policies.

A number of the administrators we spoke with indicated that they had minimal formal safety training or machine access control because they didn't believe it necessary for their space. Typically, these makerspaces had lower risk machines like 3D printers, sewing machines, or vinyl printers. P8, for example, said their space didn't need safety training at all:

"[W]e are sort of the intro low level space. So like, hey, come play with . . . 3d printing. . . " (P8)

Similarly, P2 administered a 3D printing makerspace and didn't think safety training or requirements were necessary:

"[3D printers] are pretty easy to use. So there's not . . . a lot . . . in terms of safety requirements except for you don't . . . want to touch it when it's in process, because it's really hot." (P2)

Administrators of makerspaces with more dangerous equipment tended to have stricter access control policies and mechanisms of enforcement. P13 took a hard stance on ensuring users are trained on dangerous equipment, making access contingent on safety training. They implemented their own Internet of Things (IoT) system, ensuring only those with the correct training can activate the equipment.

Trust in end-users. The third point that influenced how safety affects access control policies in makerspaces is administrators' trust in the competence of their end-users.

Even makerspaces with dangerous equipment sometimes had loose access control policies because administrators believed their users competent. P11 shared that they didn't have any specific training for equipment or restrictions for equipment usage in the space. Instead they took a passive approach, teaching equipment use when asked and relying on their users to know when to ask for help:

"[If] somebody wants to use like our table saw or a bandsaw [and is] you know not familiar with it, we'll do it for them. We don't want anybody to get hurt, a lot of people want to try it themselves and so we'll show them how to use it." (P11)

Even P13, who implemented the aforementioned IoT access control mechanism relied on user and community judgment to ensure safety:

"We have signage . . . safety equipment is kind of left out . . . [a]nd then when there is certification required . . . we go through . . . the safety processes for what people are supposed to be using. . . [I]t's also up to the community to . . . keep an eye out for each other and . . . when you see somebody doing something really sketchy to interrupt and say, 'Hey . . . can I show you maybe a safe way to do that?' " (P13)

Other makerspaces like P15 allowed 24/7 access to their end-users without surveillance or a staff member present. P13 allowed the public to access the space whenever there was a member present, while P14 allowed 24/7 access for all members. These makerspaces appear to operate on an "honor system": the administrators assume their user base is honest and competent enough to have greater access to the space.

Most (12) of the makerspace administrators we talked to, however, did not have unfettered trust in their end-users and only opened their spaces to users when staff were present. These administrators craved a solution to increase access, but only if proper safety procedures could be guaranteed. P4 and P12, both administrators of student-oriented makerspaces that were only open if staff were present, indicated their willingness to open 24/7 if they could be sure that users can maintain their "at least two people in the room" safety policy. They also showed a willingness to give some users 24/7 access if they knew that these users would respect the space. In other words,

some administrators were willing to allow individuals earn their trust, and gain privileged access, if those users demonstrated themselves worthy of such trust over time.

5.1.2 Logistics. Logistics were the second broad factor that influenced the construction of access control policies in makerspaces. We define logistics as the physical features of the space and human resources available. During our open coding process, we identified three logistical constraints that correlated with access control policies: capacity, the synchrony between staff and end-user schedules, and the staff sufficiency.

Capacity. Capacity relates to the physical size of the space and the average daily number of users of the space. We categorized makerspaces into small, medium, and large based on the number of daily users, as illustrated in Table 1. We found that administrators of larger makerspaces were more likely to automate access control.

Most administrators of medium and large makerspaces (P2, P6, P7, P9, P12, P16) reported that they implemented some form of physical authentication (e.g., a sign-in system, a card/badge/key fob system) so only makerspace members could enter the space. Administrators of smaller makerspaces usually only allowed walk-ins when staff were present in the space.

In these examples, the larger capacity of a space motivates the administrators to automate member authentication. For instance, P9, an administrator who was an active participant and leader at ISAM (a conference for academic makerspaces) [8], highlighted the difference between a small space and a large space succinctly:

"There are some shops [makerspaces] on campuses that have like 30 people in it. ... [O]ne person sits there, and they know everybody by name, who uses the space, and, you know, an access program for them compared to a shop that runs through thousands of students a semester. They're both makerspaces. We actually look ... [at] libraries on campus, because they're the ones that are using the same kind of access control, ... they're trying to get a large number of students through in an automated fashion, while still having ... control over who's coming and what they're doing." (P9)

P10, who runs a smaller makerspace with fewer than 30 daily users, provided additional evidence in support of capacity-differentiated access control policies:

"[T]he only people that have [badge] access are myself, my team, the interns, and then the mentors. So any of them can badge in and then once we get in, we unlock the doors and ... people just come in." (P10)

In addition to controlling access to the physical space, capacity also factored into the access control for individual machines. P15 mentioned their small capacity meant machines needed to be swapped, by the users themselves:

"We have an awful lot of stuff crammed into a space that's too small. We do a lot of hot swapping."(P15)

P7 provided a contrasting perspective from a makerspace with many daily active users—owing to the busyness of the space, a long queue would form around popular machines that would crowd the space. In response, they implemented a queuing and reservation system to keep the space in order:

"Someone will show up and say, hey, I got this thing I need printed for my project due tomorrow. And I go, ... right now you're looking at a five day wait to even get your turn and they go, Well, can I just skip the line? Now? ... We'll help you out if we can. And so then we try to work in that sense of flexibility." (P7)

We observed that even with the queuing system, the administrators had to handle many edge cases with users. This was all due to the non-binary nature of access control.

Synchronizing Staff and User Schedules. A second important logistical factor was the synchronicity between staff and end-user schedules. Many participating makerspaces either required staff presence, or required a chaperone to operate some machines. Conflict between staff and end-users' schedules led to reduction in end-users' access to the space, especially in university makerspaces with student staff. For instance, P1's makerspace was open 1pm-7pm Monday through Friday due to these constraints. When asked if increasing the hours of operation would help loosen such restrictions, P1 pointed out the unstable staff schedules and conflict between staff and user schedules restricted their bandwidth:

"I think it'd be hard for us to cover morning hours ... we would probably have to hire one or two more people ... if we're doing eight to five." (P1)

Though professional staff in the makerspace also conflicted with user schedules. As P11 argued, paid professionals typically do not want to stay late and keep the space open, while students want to access the space at nighttime or early morning.

"Our opening hours causes lots of heartburn. ... [A] lot of students are or they tend to shift their time ... they want to be there from like six to midnight, and ... I don't have any staff who want to work from six to midnight, working adults ... don't want to do that generally." (P11)

P10's makerspace attempted to address the schedule conflicts by hiring different types of staff: paid student interns, volunteers, and full-time professionals:

"So, ... we ... have ... three people in the space throughout the day at any given time. ... [M]yself, and then I have two interns that work part time. ... We do have some volunteers and mentors that come in and help as well. We try to find gaps during the day where we need volunteers to come in and help." (P10)

Challenges in synchronizing staff and end-user schedules also applied to machine training, which is an essential component that allows users to gain access to individual machines. P5 illustrated this challenge: after trying many different approaches to address this challenge, their makerspace chose to set up training sessions on evenings and weekends, when both users and staff were mostly available.

"The availability of the people who need training is all over the place. And then the availability of the students who are doing the training is all over the place. ... [S]o we've tried having set trainings and having students sign up for those trainings. We have done students ... request training [for] a few times and try to bundle that together. What we found most effective is to have a few set times, and then move trainings to times that are ... high availability. I think the stable one [time for training] is ... evenings and Saturdays ... [where] we have good availability both on our students, staff and on the people who need the training." (P5)

However, not all the administrators could exercise the same strategy as P5 because with most of their staff being professionals who only wanted to work till six o'clock at night, the administrators had difficulty in arranging nighttime training sessions. Overall, we found that the solution to synchronizing staff and user schedules was that the administrators needed to make access control policies tailored to the specifics of their makerspaces.

Staff Sufficiency. Extending findings from prior work [8, 14], we found that staff sufficiency, or the availability of staff to attend to end-user requests, was the third logistical point that had bearing on access control policies. For many makerspaces, access to machines was often predicated on completing a training session run by a member of the staff. However, as P16 articulated, staff members were often spread too thin to keep up with demand:

"[B]ecause we are designed to do so many different things, and ... the pressures that be want us to do even more than ... what we usually do that we're constantly spread too thin." (P16)

In turn, staff shortages could result in a backlog of users attempting to complete these training sessions, which, in turn, impinged users' access to machines.

To address access challenges from under-staffing, several makerspaces discussed modifications they made to their training requirements. P2 discussed developing a "hybrid approach" to better match staff capacity. Rather than a long in-person training session by a staff member, the initial training was administered online.

"Our training is a hybrid process because we don't have so many staff on hand at any given time. ... We're not doing classroom based instruction, ... [about] the safety and basic uses. So [we] develop it into a Canvas course so [t]hey can ... complete the online [part] self-paced. ... Once they complete the online portion, ..., they're given a assignment, ..., an in-person hands on competency test ... with a staff, [or] supervisor ... trained at a higher level on this equipment to judge whether or not they're operating safely." (P2)

Makerspaces that had sufficient staff capacity to keep up with the demand for in-person training, however, noted its benefits in helping beginners move past rookie mistakes. For example, P5 runs a makerspace staffed with five full-time professionals and around 40 student volunteers who covered in-person training and other activities. P5 noted:

"We've ... realized that if you show them [students] on the screens behind you with all this software ..., they end up getting past a bunch of ... rookie mistakes with the machines. And you [the trainer] get past ... little issues and questions ... in a more efficient way by just doing a quick [training], sometimes it's 15 minutes." (P5)

Taken together, this finding suggests that to keep up with access demands, makerspaces that are understaffed may need to make compromises that reduce their ability to teach their end-users best practices.

5.1.3 Experience. Experience was the third broad factor that influenced the creation of access control policies in makerspaces. We define experience as the prior implementation of access control policies and exposure to the limitations and successes therein. Specifically, many space administrators refined and optimized their access control policies incrementally using a process of trial and error, collecting feedback from staff and users to guide their iterative refinements [21].

For instance, to explore whether their laser cutter room needed to be permanently staffed to monitor the training sessions that gave users access control to the machines, P5 asked a staff member to test it out for a period of time:

"[W]hat we really need is somebody to go into that room and figure out how the room should be run. What is the training look like? ... [S]o [she] (an experienced electrical engineer) helped ... pull together what that experience looks like. And we realized we didn't know if we were going to need to have someone in that (laser cutter) room full time or not. We do. (We do need to have someone in the laser cutter room full time.)" (P5)

Based on that staff member's feedback, P5 realized that permanently staffing busy areas, like the laser cutter room, was necessary to facilitate access to the machines in those areas. Their original strategy was to distribute staff on demand, but with this new discovery about access control, the administrator decided to keep the busy area constantly staffed:

"The 3d printing room in the laser cutter room are permanently staff and then depending on the load of other labs going we'll have another person who's sort of roaming upstairs, electronics are some other areas so we ended up being kind of flexible depending on the demand that we're seeing" (P5)

Administrators also discussed using trial and error to refine access control policies to specific tools and machines in their makerspaces. For example, P9 had been resistant to lending out tools to

users, but due to COVID-19, they had started allowing users to lend out tool boxes, even though they hadn't figured out a good system to keep track of them yet:

"So in the past, we've been really resistant to lending stuff out. ... [N]ow ..., since corona, we have reevaluated everything we're doing and so we're actually looking into ways that we can have grab-and-go soldering kits, and other lendable tools, got general toolboxes that people would be able to check out that had ... garage tools. And so we're looking into creating those kinds of systems in order to deal with this [COVID-19]." (P9)

Some makerspaces employed scheduling and reservation mechanisms to help users gain access to specific machines. However, these mechanisms could be abused, ironically hindering access to the machines to which they were meant to facilitate access. For instance, P10, who runs a makerspace that allowed reservation for popular machines, discussed needing to add restrictions to their machine scheduling and reservation mechanisms which originally had no restrictions on how many reservations could be made.

"We see a gap and we'll ... adjust and address situations as they come. A good example is we used to have a policy on how many appointments you could, or how many 3d printers you could reserve in a day. ... And then we had ... an individual that started scheduling all six of them every day. ... [H]e had all the printers booked for an entire week and no one else was able to print. [I]t's really not fair. There's other students that need to print ... for classes. And so ... I made a policy saying you can only reserve two printers a day." (P10)

In short, we found that administrators iteratively refined access control policies through a process of trial and error based on staff and user feedback, external circumstances, and undesired exploitation of the existing policy. Static access control policies were generally unable to handle all the edge cases that could occur in real-life operations, requiring admins to craft piecemeal refinements to the policy as they gained more experience.

5.1.4 Funding. Funding was the fourth factor that drove the construction of access control policies in makerspaces. Specifically, the source of a makerspace's funding could necessitate some groups of users having privileged access to the space, in general, or to specific machines in the space [7].

For makerspaces on college campuses, the source of funding could be a specific department of the school, a specific program of the school, or the school in general. For instance, P8 explained that, because of how they were funded, their makerspace was only open to students currently enrolled in specific classes:

"[D]uring orientation, we have the students come in and type in their ID cards ... [to] give them access for the quarter. [If] [t]hey're no longer taking the class [they] don't have access ... anymore." (P8)

P11, a professor at a university that was familiar with all other makerspaces on campus, pointed out the downside of restrictive access: the strict division across departments limited users' access to tools and equipment at other spaces that might not be available at the makerspaces to which they had access:

"There are other spaces on campus with great tools, but they don't often let our students use them. ... [A]rt department has ... a professional class wood shop, ... [but]we don't have a woodshop." (P11)

Conversely, for makerspaces running on funding from the university, administrators mostly treated students from different departments equally:

"We ... constituted making space as a learning space, ... a welcoming, ... inclusive space because a lot of the spaces around [require you being] a certain department or major or with a certain lab. So it being a place where anyone can walk in [was important]." (P7)

When funding source did not necessitate privileged access to specific users, some administrators, like P4, considered privileging groups of users who might have fewer making resources at their disposal:

"[O]ur priority is not people that have the ability to go to their own area (engineering school and architecture facility). ... [W]e have to accommodate first people ... who can't go over to architecture, or you can't go over to engineering and use their equipment, because pretty much they're designated for those for that discipline. [T]hat being said, there's a lot of times those stereos or shops, because of the certain projects that are due at one time, they get overloaded and overwhelmed. And they will flow into the makerspace [the makerspace P4 works at]." (P4)

More generally, balancing equity and fairness with access against the restrictions imposed by funding sources remained an unresolved issue with access control for many of the administrators we interviewed.

5.2 RQ2: Exceptions to and Violations of Access Control Policies

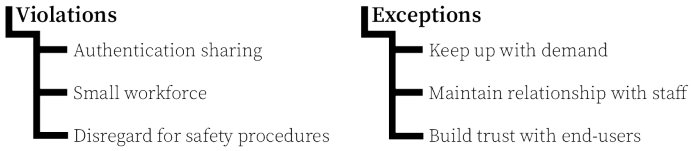

Fig. 2. Exceptions to and Violations of Access Control Policies

We next explored why and under what circumstances would administrators make exceptions to existing access control policies, as well as common violations to established access control policies that frustrated administrators. We define exceptions as deviations from an access control policy that are sanctioned by space administrators, and violations as deviations that are not sanctioned by the space administrator. Understanding these exceptional circumstances, in turn, should indicate opportunities for design. We have summarized the causes of exceptions in Fig. 2.

5.2.1 Exceptions. Many administrators took a soft-approach to enforce access control policies, making exceptions when: (i) demand for access was high; (ii) enforcing harsh policies might affect their relationship with staff; and, (iii) they built trust with the person requesting an exception.

Keeping Up with Demand. Restrictive access control policies sometimes needed to be temporarily relaxed when demand was overwhelming. For example, P1 discussed the need to allow staff into the makerspace after hours to start a backlog of 3D printing tasks to run overnight. Though their policy was to only be open between the hours of 1pm to 7pm, the workload of the makerspace led the admin to make an exception:

"When it's not one to seven [open hours], there's no one in the lab, but ... we'll have people if we have a large influx of online orders, ..., we'll have people stop in and ... start a lot of those orders. Because the machines can run overnight, you just basically need to be there for the first 10 minutes to make sure to start to correctly. But just because like the employees have the access to the lab, we'll ... use it to offset the demand during those hours by starting the online orders early to get those on time." (P1)

Maintaining Relationship with Staff. Administrators also made exceptions to their access control policies to maintain a good relationship with their staff. For example, P11 allowed his staff members to deviate from the space's access control policies, within a certain threshold, to keep his staff

happy. Specifically, he allowed staff members' friends to operate machines without proper training if the staff member was also there and if there were no safety concerns.

"Some of the staff might let their friends in . . . and let them do something that they shouldn't, but it's usually not something that's going to be life-threatening. . . . So for the most part, we are fairly [tolerant about that]. And we also want staff to be able to work and do lots of things, so we don't want to piss them off." (P11)

Similarly, P5 allowed the staff to run and monitor the space in the evening by themselves outside of normal operation hours:

"[T]here are some exemptions around access to the space in the evening. . . . [M]embers of the area lead team, we want to give them some . . . ability to open up the space. And so the policy for moving forward was that a member of the . . . leadership team needs to be sort of hall monitor for the evening hours." (P5)

P7 also said that he trusted the staff to use printers after hours when asked if any special exemptions were made to the access control policies:

"As [the staff] being part of the team, . . . if people want to like print stuff, . . . I usually say within reason like yeah, . . . go ahead." (P7)

Trust not only affected the access control policies to the physical space, but also to the specific machines and tools. P10 pointed out the trust in a mentor or a volunteer at the space would allow him to make an exception to the rule—"no tools lent out of the space":

"We don't . . . generally do that [lend tools out of the space]. Only if it's a special circumstance, . . . a mentor, or a volunteer needs to borrow something, not for the general public that comes in." (P10)

Building Trust with End-Users. Finally, some administrators also granted exceptions to end-users with whom they had built trust. This trust was mostly a function familiarity with the end-user and exposure to their objectives, as declared by P3: "If I know more about them [users] know more about what they're working on. I can sort of extend more leniency to them."

P3 also granted exceptions to people with whom they worked closely, especially faculty members:

"As a general rule, no, we don't loan equipment out. There are occasional times if it's someone that we have a closer working relationship with, especially if it's . . . one of the faculty members coming to us and asking, as opposed to just a student, we might make an exception." (P3)

Overall, in exploring administrator-sanction exceptions to access control policies, we can see that makerspace access control policies are dynamic and contextually-sensitive. Existing technical infrastructures, however, do not appear to adequately support such nuance as administrators' needed to make these exceptions manually or implicitly.

5.2.2 Violations. Sometimes, deviations from established access control policies were not sanctioned by administrators. Accordingly, we next asked administrators of instances when their access control policies were explicitly violated, and how they handled those violations.

Most of the administrators we interviewed reported that access violations at least occasionally occurred, and that it could be difficult to enforce their access control policy with some users. For instance, P10 discussed how using keycards to identify individuals and the access they should be afforded gave end-users the opportunity to lend out their keycards, which was a clear access policy violation:

" [T]he issue we have is access, so [for] students all their . . . physical access is tied to their IDs. And it's against campus policy to give your ID to anybody else. But they do. And when they do, we have systems in place that catch them, which are really advanced and they're working really well for us. But the thing that's not built into the system is okay, what happens when someone breaks a rule?" (P9)

In this case, the administrator had a way of tracking the users that violated the access control policies, but he is only able to take action after the fact instead of curbing the infraction as it was happening.

Apart from the physical access, P9 also mentioned a similar flaw in their access control method to specific machines where users could lend their access to specific machines to other people, especially those that required special training:

"By and large ... the biggest one (challenge) is that people give out their ... ID, but also a lot of our access is actually based off of their (university) authentication. So ... login is also, ... something that they give out to other people: oh, I don't have access to the laser cutter, but ... I'll get your (some other user who had access to the laser cutter) ID and your login info." (P9)

Managing access to specific tools and machines was another difficulty that administrators faced when enforcing their access control policies. Users often failed to return tools to proper places, potentially leading to access violations if other users who are not supposed to have access to the tool happened upon them. For instance, P10 discussed the struggle behind of needing to clean after users and the difficulty in tracking the users who violated the rules:

"One part of the job ... we do spend a lot of time on is picking up, you know, cleaning up after people. ... Sometimes I'm going to be working on something, we're busy helping other people and they walk out the back and left a huge mess." (P10)

Similarly, P5 pointed out that they did not have a way to constantly keep track of the whereabouts of the tools and the users that violated the tool management access policies:

"We've had one (tool station) that we put out just as sort of a test and then stuff looks like it's been stolen like. ... But then after a while we find that it's been checked in downstairs so they take it out of the tool stand upstairs and then go hand it in downstairs." (P5)

Overall, we found that end-users commonly violated makerspace access control policies, and that these violations were sometimes difficult to address. Without an effective means of tracking who is committing a violation, administrators were forced to overlook these violations.

5.3 RQ3: How Access Control Affects End-Users

Thus far, we have explored how makerspace administrators craft access control policies and navigate exceptions to the policies. Next, to address our third research question, we explore how these access control policies affect end-users interactions with the makerspace. To address this research question, we draw on the 48 survey questionnaire responses we obtained from end-users.

We found that these access control policies sometimes have untoward effects including creating inconveniences and possible security risks with regards to accessing the (i) makerspace and (ii) the machines inside of the space.

5.3.1 Access control for the makerspace. First, we explored which authentication mechanisms end-users used to access a makerspace and how those authentication mechanisms affected users' *ability* to access the makerspace. Specifically, we focused on how existing authentication mechanisms pose challenges and impose limitations on access. As we show in Fig. 3 *Graph C*, participants reported using a wide-range of authentication mechanisms: the majority used a special access card (25), while others reported paying for entry (12), using a passcode (6), or another form (2). Interestingly, 15 participants reported not needing any authentication to access their makerspace. These access methods resulted in various challenges for the user and the need for negotiable access control.

Challenges posed by existing authentication mechanisms. We asked participants to describe challenges they encountered or observed with existing mechanisms to access their makerspace. Twenty participants (41%) reported encountering challenges associated with authentication into makerspaces. In analyzing their open-ended descriptions, we uncovered two broad challenges. First,

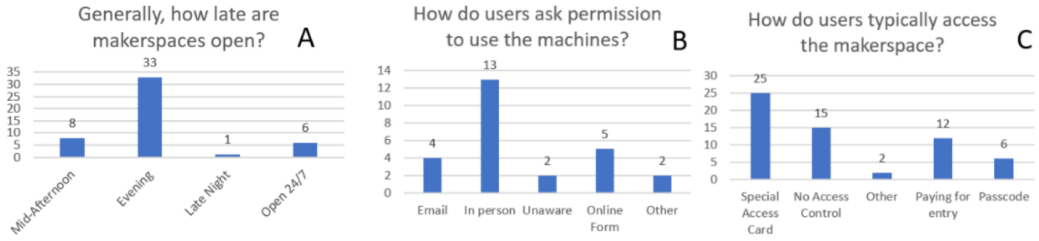

Fig. 3. Online Survey Results: (A) Answers to "Generally, how late are makerspaces open?"; (B) Answers to "How do users ask permission to use the machines?"; and, (C) Answers to "How do users typically access the makerspace?"

participants expressed concern that existing methods were insecure, as exemplified by the following response: "passcode can get leaked to non-members." Second, participants expressed a desire for a more nuanced approached to authentication that factors in social knowledge like past usage: "If students forget their access card, they are not allowed to use the machines. Regardless of past usage history."

Non-negotiability for access control. As mentioned above, makerspaces use various methods to control access to their space. We can see, in Fig. 3, a method common to all makerspaces is controlling when the space is open. However, the spaces differ on how long they remain open. Out of 48 responses, six survey results reported that the spaces were open 24/7, three of which required users to pay to access the space. Additionally, out of 33 responses which indicated that the space was only open until evening, 12 were academic makerspaces. Academic makerspaces were the ones which required a chaperone to be in the space in order for users to access it. Due to the requirements of certain projects, some require a longer time to work on, often longer than how long the space is open. This results in some issues and users of the space can only typically get access the space when it is open and/or when a chaperone is present. "After-hour entry is restricted. Once I was doing a hackathon project and was forbidden to enter the space late in the evening, while admins and lab PIs could still use the space. I hope special after-hour access can be granted to any student for a limited duration of time, like one day or a weekend."

5.3.2 Access control for individual machines. After discussing how access control policies affect end-users' ability to access the makerspace, we next asked users how these policies encumber their access to individual machines.

We found that users expressed two frustrations with how existing access control policies restrict their access to machines: redundant and unhelpful training, and slow responses to digital requests for machine access.

Redundant and Unhelpful Training. One source of frustration with existing access control policies for machine usage was that the training to use that machine was redundant or unhelpful.

Before a user is able to use a machine, they typically are required to undergo training. The purpose of this training is to teach the user how to safely use the machines. However, training for the same machine is typically similar across different makerspaces, yet there is no way for users to "transfer credit" from one makerspace to another. Six respondents (13%) felt that existing training policies were repetitive or unnecessary. When asked to embellish, one user answered: "Because I've done it before at another makerspace."

Additionally, five users (13%) stated that the training doesn't serve its intended purpose: "It feels long and most of the information gets forgotten often, I'd say to have a general information

booklet with instructions and a person to ask for more somewhere in the makerspace. With time users will get accustomed to where things are." In other words, users expressed a desire for access control to be more dynamic and contingent on immediate use rather than statically granted based on one-time training.

Slow responses to digital access requests. Another source of frustration with how access control policies affect machine usage was slow responses to digital requests for access to a machine.

Across all makerspaces, if a user wants to use a machine, they must first request access then wait in a queue. Mechanisms for requesting access varied across different makerspaces as illustrated in Fig. 3 *Graph B*: 13 users (50%) indicated that they can request access in-person while 11 (42%) indicated that they can use some form of asynchronous digital service (i.e., email, slack, or an online form). Only large makerspaces allowed the opportunity to request usage of a machine online while smaller makerspaces requested it be in person. While in-person verbal requests were often instantaneous, digital requests were often asynchronous and took a long time. In other words, there is a need for hastening responses to digital requests for machine access.

6 DISCUSSION

Generally, the administrators we interviewed shared one primary goal: to provide the greatest amount of access to their makerspaces for their users. However, we found that four practical considerations prevented makerspace administrators from affording unfettered access to their users: safety, or reducing risk of harm to users and machines; logistics, or the physical capacity and staffing constraints of the makerspace; prior experience, or situation-specific quirks that administrators have learned from trial-and-error; and, funding, or the need to provide privileged access to certain machines to certain groups of people at certain times. These four considerations formed the basis for the access control policies we uncovered in our study, but we also found evidence that existing systems for authoring and enforcing access control policies poorly map onto both administrators' and users' preferences.

We found that policy exceptions occurred regularly, with or without administrators' approval. Administrators occasionally made exceptions to maintain a good relationship with users or because they trusted a user. Sometimes, exceptions and violations to the access control policy occurred without administrator consent, usually because of a lack of effective tools.

From the end-user perspective, existing access control systems wasted time and were a cause for frustration. Users complained about the binary restrictiveness of current authentication systems (e.g., forgetting one's access card means no access at all); others found existing systems to be insecure (e.g., easily circumvented through credential sharing). Some users complained about having to repeat machine training already done elsewhere to gain access; other users thought there was not enough training repetition which could lead them to forget how to safely operate machines. Overall, we found that users had conflicting views about existing access control systems, and that few were well served by existing methods.

6.1 Implications for Design

Here, we describe a set of implications for the design of makerspace access control systems to fulfill administrator goals and to improve the end-user experience. We group the implications into two categories: contextual awareness and administrator-driven automation.

6.1.1 Contextual Awareness. Context affected administrators' ideal access control preferences, but existing systems are not expressive enough to capture these contextual variations in administrators' access preferences. Specifically, we identified four dimensions of context relevant to access control.

User Competency. User competency was an important variable in access considerations. Competency encompasses completing orientation, completing machine-specific training, and/or spending time using a machine. Records of orientation, completed training, and machine use per user would allow a context-aware approach to intelligently make dynamic access control decisions in the same way administrators allowed exceptions to static access control policies for trusted users.

Resource Availability. In our interviews with administrators, we also found that logistics were a contributing factor to access. A logging system could follow the current and historical state of the machines in the space. With this information, an intelligent access control system could optimize a schedule for users to use a tool or machine. Combined with aforementioned user metrics, it could prioritize users who historically take the least amount time on the equipment or those with the greatest need.

Safety Protocols. Safety was of great importance. A context-aware system could help ensure that proper safety procedures were being followed (e.g., wearing protective eye-wear in the wood shop) to dynamically afford access where static-policies would have denied access (e.g., too few staff on-hand). Likewise, such a system might be able to automatically stop machinery if safety protocols were violated (e.g., a second user drifting nearby without wearing safety goggles).

Negotiability. While some administrators indicated a strict adherence to following their access control policy as written, most were willing to make exceptions. An intelligent social agent with a context-aware back-end that could interact with end-users in real-time provides an opportunity to automate these negotiations. Through natural conversation, a user could provide difficult-to-sense but easy-to-verify context to an agent in order to "negotiate" for access. For example, a student could argue that a 3D print needs to be done immediately for an assignment and dynamically assess if such an exception might be allowable based on a human administrator's prior decisions in similar contexts. If the agent is not confident, it can default to the static access control policy or escalate the decision to an available human administrator.

More generally, enhancing access control systems with context awareness allows for dynamic access control policies than can evolve as social norms evolve and that can scale over busier periods of use—i.e., improve access to end-users without compromising the integrity of the access control policy.

6.1.2 Supervised Learning Agents. Most of the makerspace administrators' we interviewed adopted a digital user management system. Though administrators usually monitored these systems, they could not be available at all times to make access decisions for every user. An ideal access control solution for makerspaces must be able to automate access decision-making while preserving administrator control, allowing them to be as hands-on or as hands-off as they desire.

Anytime Administration. A makerspace can be administrated remotely through the use of IoT technologies and specialized applications. Though administrators are unlikely to accept a system that queries them for every access request, especially in the case the makerspace is kept open late. To make this approach useful for both users and administrators, it should be paired with a learning agent for simple decisions while deferring to the administrator when unsure.

Rule Generation. We found makerspace access control policies started out as common-sense rules that evolve over time with experience. A learning agent can replicate this iterative process and adapt policies to emergent social and cultural norms. Such an agent could be initialized with a set of policies borrowed from similar makerspaces and learn unique exceptions and modifications based on manual administrator decisions.

6.2 Limitations & Future Work

6.2.1 Limitations. First, survey respondents were not necessarily users of the makerspaces who's administrators we interviewed. Our initial tactic was to collect survey results via flyers in the interviewed spaces, but this proved to be untenable due to the makerspace closures that resulted from the COVID-19 pandemic. Thus, we could not make direct comparisons between user preferences and administrator decisions for a specific makerspace.

Second, user and administrator responses may have been affected by the COVID-19 pandemic. Many makerspaces were closed during data collection, so participants may not have been to a makerspace in weeks or months. This may have affected how they recalled their makerspace experiences. Additionally, many interviewees had responsibilities outside of their administrative duties and may have shifted focus to other responsibilities.

Finally, since we used a snowball sampling approach, our sample primarily (but not exclusively) consisted of people who administrated or used university makerspaces. Thus, many of our findings and recommendations may be most relevant to university makerspaces.

6.2.2 Future Work. We foresee two compelling directions for future work. First, this work can be extended through in-situ observational studies of makerspace access control. These observations would help further improve our understanding of access control breakdowns in makerspaces as they occur in practice. Second, we foresee a fruitful design space for improving access control systems in makerspaces by making them more intelligent, context-aware and interactive.

7 CONCLUSION

We conducted a mixed-methods, multi-stakeholder investigation into how makerspace administrators construct, refine, and make exceptions to access control policies, and how those policies impact end-user experiences. Specifically, we conducted a semi-structured interview with 16 makerspace administrators and a survey with 48 makerspace end-users. We found makerspace administrators were forced to craft and constantly refine static access control policies based on four dynamic and contextually-sensitive factors: safety, logistics, experience and funding. Owing to these dynamic inputs and static outputs, administrators often had to make exceptions to their policies to account for social considerations (e.g., their trust in certain end-users and their desire to maintain a good working relationship with staff). We also found end-users expressed frustration with the static and binary nature of existing access control mechanisms in makerspaces, yearning for systems more socially and contextually aware. Finally, we proposed a number of design opportunities for the development of novel access control systems for shared physical spaces.

ACKNOWLEDGMENTS

This paper was generously funded, in part, by NSF SaTC Award #1755625. We would also like to thank the makerspace administrators we interviewed for volunteering their time to speak with us.

REFERENCES

[1] [n.d.]. Otter Voice Meeting Notes. https://otter.ai Library Catalog: otter.ai.

[2] Lujo Bauer, Lorrie Faith Cranor, Robert W. Reeder, Michael K. Reiter, and Kami Vaniea. 2008. A user study of policy creation in a flexible access-control system. In *Proceeding of the twenty-sixth annual CHI conference on Human factors in computing systems - CHI '08*. ACM Press, Florence, Italy, 543. https://doi.org/10.1145/1357054.1357143

[3] Vincent Bonneau, Tiana Ramahandry, Laurent Probst, Bertrand Pedersen, and Lauriane Dakkak-Arnoux. 2017. Secure Access Control: Smart ID Management for Building Access. https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Secure%20access%20control%20v1.pdf

[4] Julie Darwin, Mr Joseph Patrick Kale, Michael S Thompson, MA Vigeant, and A Cheville. 2016. MAKER: A Maker Space Smart Badging System. In *ASEE Annual Conference & Exposition, New Orleans, Louisiana*, Vol. 10. 25600.

[5] E Davies, R Morris, and A Jariwala. 2017. Trust as the Foundation for a Successful Balance of Power in a Student Run Academic Makerspace. In *Proceedings of the International Symposium of Academic Makerspaces (ISAM)*.

[6] Serge Egelman, Andrew Oates, and Shriram Krishnamurthi. [n.d.]. Oops, I did it again: mitigating repeated access control errors on facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2011-05-07) *(CHI '11)*. Association for Computing Machinery, 2295–2304. https://doi.org/10.1145/1978942.1979280

[7] Craig R Forest, Roxanne A. Moore, Amit S. Jariwala, Barbara Burks Fasse, Julie Linsey, Wendy Newstetter, Peter Ngo, and Christopher Quintero. 2014. The Invention Studio: A University Maker Space and Culture. *Advances in Engineering Education* Summer 2014 (2014), 32.

[8] Joey A Gottbrath and Ian C Charnas. 2019. Makerspace Staffing Models: A Survey. In *Proceedings of ISAM 2019*. Yale University, 7.

[9] Sang-Yeal Han, Jaeheung Yoo, Hangjung Zo, and Andrew P. Ciganek. 2017. Understanding makerspace continuance: A self-determination perspective. *Telematics and Informatics* 34, 4 (July 2017), 184–195. https://doi.org/10.1016/j.tele.2017.02.003

[10] Ramy Imam, Leonard Ferron, and Amit S Jariwala. 2018. A Review of the Data Collection Methods Used at Higher Education Makerspaces. In *Proceedings of ISAM 2018*. Co-hosted Standford and UC Berkeley, 7.

[11] Amit Jariwala, Tim Felbinger, Thomas L. Spencer, Veronica Spencer, and Priyesh B. Patel. 2019. Safety in a Student-Run Makerspace via Peer-to-Peer Adaptive Training. *IJAMM* 1, 1 (Oct. 2019). https://doi.org/10.21428/70cb44c5.c9986b05

[12] Kyungwon Koh and June Abbas. 2015. Competencies for Information Professionals in Learning Labs and Makerspaces. *Journal of Education for Library and Information Science Online* 56, 2 (2015), 114–129. https://doi.org/10.12783/issn.2328-2967/56/2/3

[13] Gabriel Licks, Adriano Teixeira, and Kris Luyten. 2018. Smart Makerspace: A Web Platform Implementation. *International Journal of Emerging Technologies in Learning (iJET)* 13, 02 (Feb. 2018), 140–156. https://online-journals.org/index.php/i-jet/article/view/7904

[14] Robert D Mabry, Suzanne M Valery, and Brie J Lindsey. 2018. Santa Maria's Central Coast Makerspace Collaborative: A Network of Internal and External Partners. In *Proceedings of ISAM 2018*. Co-hosted Standford and UC Berkeley, 7.

[15] 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. [n.d.]. Access Control for Home Data Sharing: Attitudes, Needs and Practices. ([n. d.]), 10.

[16] Alexis Noel, Lauren Murphy, and Amit S Jariwala. 2016. Sustaining a diverse and inclusive culture in a student run makerspace. In *Proceedings of ISAM 2016*.

[17] Sofia Papavlasopoulou, Michail N Giannakos, and Letizia Jaccheri. 2017. Empirical studies on the Maker Movement, a promising approach to learning: A literature review. *Entertainment Computing* 18 (2017), 57–78. Publisher: Elsevier.

[18] Tara Radniecki and Mitch Winterman. 2020. Leveraging student expertise for niche services. *Reference Services Review* ahead-of-print, ahead-of-print (Jan. 2020). https://doi.org/10.1108/RSR-11-2019-0083

[19] Robert W Reeder, Lujo Bauer, Lorrie F Cranor, Michael K Reiter, and Kami Vaniea. 2011. More than skin deep: measuring effects of the underlying model on access-control system usability. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2065–2074.

[20] Talia Ringer, Dan Grossman, and Franziska Roesner. [n.d.]. AUDACIOUS: User-Driven Access Control with Unmodified Operating Systems. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (New York, NY, USA, 2016-10-24) *(CCS '16)*. Association for Computing Machinery, 204–216. https://doi.org/10.1145/2976749.2978344

[21] Dustyn Roberts and Jenni Buckley. 2020. Case Study: Maker Space Management by Minions. *Advances in Engineering Education* Spring 2020 (2020), 11.

[22] Eldon Schoop, Forrest Huang, Nathan Khuu, and Bjoern Hartmann. 2018. MakerLens: What Sign-In, Reservation and Training Data Can (and Cannot) Tell You About Your Makerspace. In *Paper presentation, International Symposium on Academic Makerspaces, Stanford, CA, August*.

[23] Thomas Wildbolz, Hans P. Schnöll, and Christian Ramsauer. [n.d.]. Managing Access to Space, Tools, and Machines at the Schumpeter Laboratory for Innovation. In *Proceedings of ISAM 2019*. Yale University, 6.

[24] Megan E Tomko, Julie Linsey, Robert Nagel, and Melissa W Alemán. 2017. Exploring meaning-making and innovation in makerspaces: An ethnographic study of student and faculty perspectives. In *2017 IEEE Frontiers in Education Conference (FIE)*. 1–9. https://doi.org/10.1109/FIE.2017.8190580

[25] Scooter Willis. [n.d.]. The Maker Revolution. 51, 3 ([n. d.]), 62–65. https://doi.org/10.1109/MC.2018.1731074

A SEMI-STRUCTURED INTERVIEW QUESTIONS

A.1 Demographic Questions:

- What gender do you identify as?
- What is your age?
- What is the name of the makerspace you are in charge of?
- Is there a specialty for the makerspace?
- How long have you been in this role?

A.2 Interview Questions

- This question was designed to know the identity of the administrators.
  - Is this your primary job function?
- The following questions were designed to understand the factors that affect the management of the space.
  - What would you say is the simplest part of your job?
  - What would you say is the most difficult part of your job?
- This question was designed to understand how the administrators manage the space on a daily basis.
  - What do you spend the most time on during the day?
- This question was designed to evaluate the busyness of the makerspace to compare administrators' perception and the users' perception.
  - How many people on average do you think you have in the space on any given day?
- The following questions were designed to understand how the staff can affect the management of the space.
  - Do you staff mainly with volunteers or do you hire employees?
  - Roughly, how many (volunteers/employees) do you have working with you during each shift?
- The following questions were designed to understand the strengths of different factors influencing the management of the space.
  - What do you think are the most important policies you have for the space? Why?
  - What do you think are the least important policies you have for the space? Why?
- The following questions were designed to understand the effectiveness of the current policies.
  - How do you feel the volunteers do in keeping policies consistent?
  - Do you feel your policies are well enforced?
  - Do you feel your policies can be too harshly enforced?
- This question was designed to understand how the administrators create and manage their policies in managing the makerspace.
  - How do you define your policies?
- This question was designed to understand how safety contributes to the management of the makerspace.
  - What do you do to ensure the safe usage of machinery?
- This question was designed to understand the exemptions made during management of the makerspace.
  - Do you have any special exemptions from policies or are they uniform across the board?

B SEMI-STRUCTURED INTERVIEW CODEBOOK

Code Name	Definition	Frequency	Exemplary Quotes
Safety: Individual Judgement	Situations when an administrator balances between access and safety based on personal judgment	11	"The most important thing is safety . . . , but I put culture in front of that because it includes safety, but it also includes other things like how you operate in the space, how you serve the community." (P6) "Safety is important enough to require training on each piece of machinery and close parts of space when aren't enough staff to support keeping everything open." (P7) "We make everybody who comes in, whether or not they are a member, . . . to sign a liability waiver which essentially says we have done everything. We have made reasonable efforts to keep you safe. Everything we've done with with the we're keeping the tools sharp and maintained. We're providing all of the safety requirement. If you do not use it that is entirely on you." (P16)
Safety: Machine Danger	Situations where an administrator designs access policies based on the danger level of the machines in the space.	8	"So we have training that's required for those things (machines) that have special safety concerns." (P13) "Most of the equipment is relatively safe, . . . the worst thing happened with a 3d printer you can get burned . . . on your finger or something . . . ." (P4)
Safety: Trust in End-Users	Situations where the administrators create access control policies based on their level of trust in their users.	16	"Safety is the responsibility of the user(s), people should be able to use the space safely without much guidance." (P16) "I would prefer . . . [if] there's more than one person in the lab. [In that case], since the building that our makerspace is located in, does have a 24 hour security officer. . . . I think having 24 hour open lab is preferable if someone for whatever reason needs to be working at 1am I'd much rather them be able to do their work because at that point, they're probably kind of desperate to get it done right then." (P3)

Table 3. Interview Safety Codes

Code Name	Definition	Frequency	Exemplary Quotes
Logistics: Capacity	Situations where the physical size of the space and average daily number of users the different authentication methods the administrators adopt	10	"If [a user] says I want to use the laser cutter, [staff] look on the cameras to see if the laser cutters are available. . . . And if they [the users] need help, [staff] can hop on a walkie talkie and let one of our second floor staff know somebody's going to need some guidance on laser in a moment." (P2) "We're only open until four because one of the professor's has class [that is hosted in the makerspace] from five to eight. . . . We're typically closed during those hours [class time], . . . because we can't really fit more than like 20 [people] in our labs, and the classes usually have around 15 people." (P1)
Logistics: Synchronize Schedules	Situations where administrators struggle to resolve conflicts between staff and user schedules	9	"Our opening hours causes lots of heartburn. . . . [A] lot of students are or they tend to shift their time . . . they want to be there from like six to midnight, and . . . I don't have any staff who want to work from six to midnight, working adults . . . don't want to do that generally." (P11) "[On] Wednesday nights we usually get more than 30 entries. . . . So they (staff) hold office hours . . . where we're leaving the door unlocked from 7pm till 9pm." (P14) "We have to hire so many [staff], even though there's only two or three [staff in the space] at a time . . . [S]tudent schedules . . . are varying and changing all the time. [T]o get people available for our shifts . . . , we need quite a few people and some redundancy. On weekends, the staff are there by themselves." (P4)
Logistics: Staff Sufficiency	Situations where the amount of staff available to the makerspaces affect the access control policies of the space	5	"Our training is a hybrid process because we don't have so many staff on hand at any given time . . . . We're not doing classroom based instruction, . . . [about] the safety and basic uses. So [we]develop it into a Canvas course so [t]hey can . . . complete the online [part] self-paced . . . . Once they complete the online portion, . . . , they're given a assignment, . . . , an in-person hands on competency test . . . with a staff, [or] supervisor . . . trained at a higher level on this equipment to judge whether or not they're operating safely." (P2)

Table 4. Interview Logistics Codes

Code Name	Definition	Frequency	Exemplary Quotes
Exception: Keeping up with Demand	Describe situations where demand for access is high that leads the administrators to make exceptions to their access control policies	4	"So [we] starts off a very high frequency of trainings. And then we would gradually diminish that till the halfway point of the semester. And then we cut off those ...hands-on trainings. We try to focus the second half of the semester on just helping people with their projects. Our busiest time is the end of the semester." (P9) "We try to get our staff to operate in many ways. ...We've said, hey there's some issues that we have, but we want you guys [staff] to solve it and we had some late evening hours access that ...we provided to our students staff in December." (P5) "The simplest part of my job is helping people in the maker space. So I'm available for people who need training on things, who want an orientation to the lab and stuff like that." (P4)
Exception: Maintaining Staff Relationship	Describe situations where the administrators make exceptions to access control policies to maintain good relationship with staff	2	"[T]here are some exemptions around access to the space in the evening. ...[M]embers of the area lead team, we want to give them some ...ability to open up the space. And so the policy for moving forward was that a member of the ...leadership team needs to be sort of hall monitor for the evening hours." (P5) "As [the staff] being part of the team, ...if people want to like print stuff, ...I usually say within reason like yeah, ...go ahead." (P7)
Exception: Building End-User Trust	Describe situations where the administrators make exceptions to access control policies because of the trust they have in the end-users	3	"As a general rule, no, we don't loan equipment out. There are occasional times if it's someone that we have a closer working relationship with, especially if it's ...one of the faculty members coming to us and asking, as opposed to just a student, we might make an exception." (P3) "So ...there are some things about like, like electrical safety that I went through with him [a person that comes to the space often]. And basically the rule was no working with AC power , [and] ...power from the wall outlet. Unless there were at least two people around ...and they knew what they were doing so." (P11)

Table 5. Interview Exception Codes

Code Name	Definition	Frequency	Exemplary Quotes
Violations	Describes situations where the users violate the access control policies in place	10	"[I]t's like a trust system where students would borrow it to use it in on site, and then they would just have to put it back. So we don't have a way to keep track [of where the tools are]. So one of the problems is that students sometimes do lose it and if ever they break it, and we don't know who broke it." (P8) "Things are an absolute absolute mess. If the staff are not needed at the front desk, ... [we] will have them ... going and tracking down all the wrenches or all the screwdrivers or whatever and putting everything back, or doing inventory with our materials and back and storage and that kind of stuff. And so, ... that is a huge struggle." (P6)
Experience	Situations where the prior implementation of access control policies and exposure to the limitations and successes therein affect the access control polices of the space	6	"I've allowed some small hand tools and stuff [to be lent out] ... [But] sometimes it's challenging to keep track when you have so many students that come in, and you are constantly multitasking. So I have adapted to send emails to remind students ... by the end of semester." (P4) "One of our policies is no unauthorized donations. And this is ... something that's gradually ratcheted up ... over the years, but it's gotten to the point now where literally, you cannot leave anything at Tinker mill that you brought, unless I [the administrator] personally have approved it. ... [This is because] we had an awful lot of people just dumping stuff on us." (P12)
Funding	Situations where the source of funding could necessitate some groups of users having privileged access to the space or to specific machines in the space	5	"We ... constituted making space as a learning space, ... a welcoming, ... inclusive space because a lot of the spaces around [require you being] a certain department or major or with a certain lab.So it being a place where anyone can walk in [was important]." (P7) "I think it would be cool ... to be open you know, like later at night or on Sunday, for example. ... We ... used to be open till nine o'clock at night. ... And when you looked at that eight to nine hour, there were so few people utilizing the library versus the expense of keeping the building open for an extra hour. It just didn't make sense." (P13)

Table 6. Other Interview Codes

C SURVEY QUESTIONNAIRE

C.1 Informed Consent

Participants were provided with information related to the study and either selected "I consent, begin the study" or "I do not consent, I do not wish to participate"

C.2 Raffle

Participants were asked if they wanted to be entered into a raffle for $25 and depending on the answer, were taken to the page with the link.

C.3 Demographics

The following questions were designed to obtain the demographics of our participants:

- What is your gender?
  - Male
  - Female
  - Other
- What is your age?
  - 18-24
  - 25-34
  - 35-44
  - 45-54
  - Over 55
- What is your ethnicity?
  - White
  - Black or African American
  - American Indian or Alaska Native
  - Asian
  - Native Hawaiian or Pacific Islander
  - Other
- What is the highest degree or level of school you have completed?
  - Less than a high school diploma
  - High school degree or equivalent
  - Bachelor's degree (e.g. BA, BS)
  - Master's degree (e.g. BA, BS)
  - Doctorate (e.g. PhD, EdD)
  - Other
- What is your current employment status?
  - Employment full-time
  - Employed part-time
  - Unemployed
  - Student
  - Retired
  - Self-employed
  - Unable to work

C.4 About the Makerspace

The following questions were asked to learn more general information about the makerspaces our participants were familiar with:

- This question was designed to determine how many makerspaces the participant was familiar with.
  - Do you visit more than one makerspace?
    - Yes
    - No
- This question was designed to learn if multiple participants were reporting about the same makerspace.
  - What is(are) the name(s) of the makerspaces you visit?
- This question was designed to determine if location would factor into any of our findings.
  - What is(are) the location of these makerspaces? (Name of the institution(s) or company(s))
- This question was designed to understand how familiar the participant was with the makerspace.
  - How often do you access the makerspaces overall? (Number of hours per week)
    - 0-2
    - 2-4
    - 4-6
    - 6-8
    - 9+
- This question was designed to determine if the hours of the makerspace would factor into any of our findings.
  - Generally, how late are the makerspaces open?
    - Mid-afternoon
    - Evening
    - Late Night
    - Open 24/7
- This question was designed to determine if the hours a user could access the makerspace would factor into any of our findings.
  - Are there limits to the number of hours you can access the makerspaces?
    - 3-6 hours / week
    - 6-9 hours / week
    - 9+ hours / week
    - No limits
    - Other
- This question was designed to determine the purpose of the makerspace
  - What do you usually do in the makerspaces?
    - 3D Printing
    - Laser Cutting
    - Wood Work
    - Soldering
    - Studying
    - Other

C.5 Busyness and Interactions

The following questions were designed to both determine how busy the makerspace typically is and what are the various roles of people in the makerspace:

C.5.1 Busyness.

- How busy do you feel the makerspace(s) is/are during your usual visiting times?

  - Very busy
  - Slightly busy
  - Not very busy
  - Not busy at all
- Do the machines you want to access typically have a long queue?
  - Always
  - Most of the time
  - About half the time
  - Sometimes
  - Never
- Please name the machines that typically have a long queue.

C.5.2 Interactions.

- Who do you usually interact with when you are in a makerspace? (Select All That Apply)
  - Administrator
  - Volunteers (eg. PI)
  - Fellow users
  - No one
  - Other
- How often do you interact with the admin of a makerspace?
  - Always
  - Most of the time
  - About half the time
  - Sometimes
  - Never
- What do you usually discuss with the admin?
- How often do you interact with the volunteers of a makerspace?
  - Always
  - Most of the time
  - About half the time
  - Sometimes
  - Never
- What do you usually discuss with the volunteers?
- How often do you interact with the fellow users of a makerspace?
  - Always
  - Most of the time
  - About half the time
  - Sometimes
  - Never
- What do you usually discuss with the fellow users?

C.6 Access Authentication

The following questions were designed to understand how different makerspaces structured their access control:

- This question was designed to determine how first-time users access the makerspace.
  - How did you gain access to makerspace(s) for the first time? (Select All That Apply)
    - Signing a waiver
    - Getting special access card

    * Paying for entry (e.g., subscription, single entry cost)
    * Going through orientation
    * Passcode
    * No Access Control
    * Other
- This question was designed to understand how makerspaces give access to their users.
  - How do you usually access the makerspace(s)? (Select All That Apply)
    * Special access card
    * Paying for entry (e.g., subscription, single entry cost)
    * Passcode
    * No Access Control
    * Other
- This question was designed to determine if a user has accessed multiple makerspaces, to see if orientation is redundant.
  - For each makerspace, did you have to re-do orientation or obtain a different access card?
    * Yes
    * No
- This question was designed to determine if the user has trouble with the current access method.
  - Are you able to access a makerspace without trouble using the current authentication method?
    * Yes
    * No
- This question was designed to determine what troubles a participant had, if any.
  - Please briefly describe how the current authentication method has caused any trouble, and if possible, some suggestions to improve the current method.

C.7 Training

The following questions were designed to understand how different makerspaces structured their training methods in order to allow participants to use their machines:

- Select the following that apply to machine usage in makerspaces you frequent
  - Special Training is required (some/all)
  - Chaperone is required (some/all)
  - Special permission is required (some/all)
- Have you ever felt that the special training is repetitive or unnecessary?
  - Yes
  - No
- Please briefly describe why you felt the special training is repetitive or unnecessary, and if possible, give some suggestions.
- How clear are your special training requirements?
  - Extremely clear
  - Moderately clear
  - Slightly clear
  - Neither clear nor unclear
  - Slightly unclear
  - Moderately unclear
  - Extremely unclear

- After the special training, how comfortable are you with operating the machines?
  - Extremely comfortable
  - Moderately comfortable
  - Slightly comfortable
  - Neither comfortable nor uncomfortable
  - Slightly uncomfortable
  - Moderately uncomfortable
  - Extremely uncomfortable

C.8 Chaperones

The following questions were designed to understand how various makerspaces structure their chaperone policy and to see what the responsibilities of chaperones are:

- Who is usually the chaperone?
  - Administrator
  - Volunteers (eg. PI)
  - Other
- Is chaperone required for some machines or all machines?
  - Some machines
  - All machines
- Please name the machines that require a chaperone to use.
- Are you able to use machinery in the makerspace(s) without trouble under the current chaperone protocol? (eg. Any issues such as chaperone not present)
  - Yes
  - No
- Please briefly describe how the current chaperone protocol has caused any trouble, and if possible, some suggestions to improve it.

C.9 Permissions Protocol

The following questions were designed to understand what permissions must the user receive in order to use various aspects of the makerspace and if any of these are hindering their usage:

- Please name the machines that require special permission to access.
- How can you ask for the permissions to use the machines?
  - Email
  - In person
  - Online Form
  - Unaware
  - Other
- Who do you ask for special machine usage permissions?
  - Administrator
  - Volunteers (eg. PI)
  - Unaware
  - Other
- How long does it take to receive a response?
  - Immediate
  - Within the hour
  - Within the day
  - Within the week

  - Longer
- Are you able to access the machines you'd like to use without trouble under the current permissions protocols?
  - Yes
  - Maybe
  - No
- Please briefly explain a situation where you had trouble accessing the machines under the current permission protocols and if possible, some of the suggestions you have for the current protocols.

C.10 Specific Scenarios

The following questions were designed to determine how likely a specific access control situation was to occur:

- Someone is looking for advise from their supervisor. Although the supervisor is present, the door to the office is closed.
  - Extremely likely
  - Moderately likely
  - Slightly likely
  - Neither likely nor unlikely
  - Slightly unlikely
  - Moderately unlikely
  - Extremely unlikely
- A student working with a professor needs to have a document signed. While the student has contacted the professor beforehand, the professor is busy at the moment and has the door closed.
  - Extremely likely
  - Moderately likely
  - Slightly likely
  - Neither likely nor unlikely
  - Slightly unlikely
  - Moderately unlikely
  - Extremely unlikely
- A student in a professor's class is looking to speak with them to discuss an assignment during office hours. The professor is not present (held at another meeting), but the student is not aware of that.
  - Extremely likely
  - Moderately likely
  - Slightly likely
  - Neither likely nor unlikely
  - Slightly unlikely
  - Moderately unlikely
  - Extremely unlikely
- A student who left some belongings in the maker space wants to pick it up (the student sent the admin an email about this, and admin agreed to be here), but admin is not here due to another meeting. Currently, the student does not have access to the maker space because it is outside their assigned hours.
  - Extremely likely

  - Moderately likely
  - Slightly likely
  - Neither likely nor unlikely
  - Slightly unlikely
  - Moderately unlikely
  - Extremely unlikely
- Someone suspicious is wandering around the maker space.
  - Extremely likely
  - Moderately likely
  - Slightly likely
  - Neither likely nor unlikely
  - Slightly unlikely
  - Moderately unlikely
  - Extremely unlikely
- A past student forgot their papers when visiting a professor, and has come back for it. However, the professor is not here, and the student is not certain when the professor will be back.
  - Extremely likely
  - Moderately likely
  - Slightly likely
  - Neither likely nor unlikely
  - Slightly unlikely
  - Moderately unlikely
  - Extremely unlikely

D SURVEY CODEBOOK

Code	Definition	Frequency	Exemplary Quotes
Insecure	Current authentication methods are seen as insecure to users	3	"Passcode can get leaked to non-members." "We had a problem with the passcode being very low tech 4 digit code, that was shared too widely in an unauthorized manner." "It only works on the front door."
Inconvenient	Current authentication methods hinder uses or are inconvenient to users	9	"Sometimes the access card is down. It's down frequently enough that now I just use the passcode that is emailed once a month." "Sometimes it takes ages for the buzzcard office to reflect that you have access and allow the door to open with the buzzcard" "Every makerspace seems to have its own home-grown solution that only one person who's no longer a member remembers how to fix."
Non-Negotiable	Current authentication methods are binary, and are not adaptive to different situations happening	5	"Can't access the shop on the weekend." "After-hour entry is restricted. Once I was doing a hackathon project and was forbidden to enter the space late in the evening, while admins and lab PIs could still use the space." "If students forget their access card, they are not allowed to use the machines. Regardless of past usage history"
Redundant Training	Current training methods are seen as repetitive or redundant	6	"Because I've done it before at another makerspace"
Unsuccessful Training	Current training methods don't serve their proper purpose	5	"It feels long and most of the information gets forgotten often" "Feels like over caution."

Table 7. Survey Codes