Tensions between Access and Control in Makerspaces

By Jacob Logas, Ruican Zhong,
Stephanie Almeida,
Sauvik Das

Faculty Member #1:

Printed: Sauvik Das
Signature: Sauvik Das

Faculty Member #2:

Printed: Rosa Arriaga
Signature: 

1
1 ABSTRACT
Makerspaces refer to highly interactive physical spaces where people can work on projects. These spaces 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 multi-stakeholder study where we consider opinions from both the administrators and the users of the spaces. Specifically, we conducted 16 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.

2 INTRODUCTION
Access control is the mechanism through which permissions to a resource — either physical or digital — are granted or denied. It 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 [7], most spaces default to a binary access dichotomy, relying mainly on card-based systems (71%) [2].

Prior work suggests existing digital access control mechanisms for shared spaces map poorly onto real-world access needs [1]. Prior work also highlights that existing access control systems are often ambiguous, which can cause conflicts that are difficult to resolve and can result in unintended access [8]. 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 an investigation into the dual perspectives of space administrators and end-users with respect to access control in the context of makerspaces.

Makerspaces refer to highly interactive physical spaces where people can use tools and technology (e.g. hand tools, 3D printers, laser cutters etc.) to collaborate on various projects. Some are often supported by high schools and universities, where students would work on course projects or personal projects. Other commercial ones are often supported by their subscribers who work on personal projects in the space. These spaces 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 [3, 4, 6, 9].

We performed 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.

3 METHODOLOGY

We ran an investigation consisting of two studies. 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. We provide the full interview questions and survey questionnaire in this paper for review.

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. At the beginning, the administrators were asked to provide demographic data. Once completed, we asked them 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.

By inquiring using an open conversation format, we were able to gain intimate information about the specific makerspaces and the interviewees. During the interviews, we had the privilege to know the administrators on a personal level. Additionally, we often followed up with questions that would focus on the administrators’ past experiences and personal preferences regarding policy making and enforcement. Therefore, we gained more context information to understand not only the choices the administrators made regarding the access control policies, but also the different factors that influenced their decisions.

3.1.2 Recruitment In creating a list of potential participants, 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.

3.1.3 Analysis For the purpose of analysis, we recorded and transcribed the interviews. Then, two researchers extracted excerpts relevant to the research questions and independently tagged each excerpt with a keyword to represent the theme of the information. These two researchers came together to discuss their independent tags until settling on a final version. The final version had 12 tags 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 analyze the remaining excerpts. This method helped ensure different opinions regarding each excerpt and each theme to be incorporated throughout the analysis process. Afterwards, we calculated descriptive statistics based on the 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. Due to our need for descriptive statistics regarding user experience instead of detailed reasoning, we employed an online questionnaire. This 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.

---

2Pilot interviews are test runs to evaluate and improve the feasibility and cost of the interviews. Note that the results of these interviews are not included in the final results.
3.2.1 Procedure To participate in the study, the users filled out a Qualtrics\textsuperscript{3} 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.

3.2.3 Analysis After participants filled out the survey, we analyzed and graphed the results of the multiple choice questions to see where the trends were. We then extracted themes from the free response questions asked in the survey using a method similar to the interview results. Two researchers extracted excerpts related to our third research question. The excerpts were then assigned to corresponding themes for analysis purposes.

Amongst the free response questions, we focused on questions relating to access control of the space, \textit{How do you usually access the makerspace?}, \textit{Are you able to access a makerspace without trouble using the current authentication method?} with a followup question of \textit{Please briefly describe how the current authentication method has caused any trouble, and if possible, some suggestions to improve the current method.}, \textit{Generally, how late are the makerspaces open?}. We also looked at responses regarding access control to machines, specifically asking \textit{Have you ever felt the special training is repetitive or unnecessary} with a followup question of \textit{Please briefly describe why you felt the special training is repetitive or unnecessary, and if possible, give some suggestions.} and \textit{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.

4 DATASET

4.1 Interview data

We conducted 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).

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

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

\textsuperscript{3}an online platform hosting surveys
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)

<table>
<thead>
<tr>
<th>Gender</th>
<th>Full-Time</th>
<th>Population</th>
<th>Size</th>
<th>For Profit</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>Female</td>
<td>College Students &amp; Faculty</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>P2</td>
<td>Male</td>
<td>College Students &amp; Faculty</td>
<td>Large</td>
<td></td>
</tr>
<tr>
<td>P3</td>
<td>Male</td>
<td>College Students</td>
<td>Small</td>
<td></td>
</tr>
<tr>
<td>P4</td>
<td>Male</td>
<td>College Students</td>
<td>Large</td>
<td></td>
</tr>
<tr>
<td>P5</td>
<td>Male</td>
<td>College Students</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>P6</td>
<td>Male</td>
<td>College Students &amp; Faculty</td>
<td>Large</td>
<td></td>
</tr>
<tr>
<td>P7</td>
<td>Male</td>
<td>College Students, K12 Students</td>
<td>Large</td>
<td></td>
</tr>
<tr>
<td>P8</td>
<td>Female</td>
<td>College Students</td>
<td>Small</td>
<td></td>
</tr>
<tr>
<td>P9</td>
<td>Male</td>
<td>College Students</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>P10</td>
<td>Male</td>
<td>College Students, Community</td>
<td>Small</td>
<td></td>
</tr>
<tr>
<td>P11</td>
<td>Male</td>
<td>College Students</td>
<td>Large</td>
<td></td>
</tr>
<tr>
<td>P12</td>
<td>Male</td>
<td>Community</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>P13</td>
<td>Female</td>
<td>Community</td>
<td>Small</td>
<td></td>
</tr>
<tr>
<td>P14</td>
<td>Male</td>
<td>Community</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>P15</td>
<td>Female</td>
<td>Community</td>
<td>Small</td>
<td></td>
</tr>
<tr>
<td>P16</td>
<td>Male</td>
<td>Community</td>
<td>Large</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Gender</th>
<th>18-24</th>
<th>25-34</th>
<th>35-44</th>
<th>45-54</th>
<th>Student</th>
</tr>
</thead>
<tbody>
<tr>
<td>Female</td>
<td>50%</td>
<td>31.25%</td>
<td>14.58%</td>
<td>4.17%</td>
<td>Employed Full-time</td>
</tr>
<tr>
<td>Male</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>31.25%</td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Employed Part-time</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.42%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Self-Employed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4.17%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Unemployed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4.17%</td>
</tr>
</tbody>
</table>

Table 2. Demographics of online survey participants

Fig. 1. Factors that influenced Access Control Policies

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 [3]. 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. 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.

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 because it was an intro low level space. Similarly, P2 administered a 3D printing makerspace and didn’t think safety training or requirements were necessary.

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

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. 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) [4], 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)

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.

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.

Overall, 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.

Professional staff schedules 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.

To address the schedule conflicts, P10 started hiring different types of staff: paid student interns, volunteers, and full-time professionals.

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.

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 [4, 6], 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 because the space was designed to do so many different things. 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 and users can work on that self-paced. This greatly reduced the amount of time each hands on training session would take.

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 [9].
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. 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.

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.

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. This was due to some people scheduling all the 3d printers for a week, which was an unfair situation for other students who needed the machines.

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 [3].

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.

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. Conversely, for makerspaces running on funding from the university, administrators mostly treated students from different departments equally, as P7 mentioned. 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.

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

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 exceptions from time to time to handle a large influx of orders.

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. 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.

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.”

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 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 of needing to clean after users and the difficulty in tracking the users who violated the rules. 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.

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, 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 approach 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.

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 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 Limitations & Future Work

**6.1.1 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, 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.

6.1.2 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. This design space holds potential for changing the ways people, both the administrators and the users, interact with each other and with the access control systems.

7 CONCLUSION

We conducted a 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 interviews 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. With these results, we foresee further observational studies of makerspace access control and potential design opportunities for the development of novel access control systems for shared physical spaces.

REFERENCES

