Optimistic Access Control for the Smart Home

Nathan Malkin, Alan F. Luo, Julio Poveda, Michelle L. Mazurek
University of Maryland

***Abstract*—One of the biggest privacy concerns of smart home users is enforcing limits on household members' access to devices and each other's data. While people commonly express preferences for intricate access control policies, in practice they often settle for less secure defaults. As an alternative, this paper investigates "optimistic access control" policies that allow users to obtain access and data without pre-approval, subject to oversight from other household members. This solution allows users to leverage the interpersonal trust they already rely on in order to establish privacy boundaries commensurate with more complex access control methods, while retaining the convenience of less secure strategies. To evaluate this concept, we conducted a series of surveys with 604 people total, studying the acceptability and perceptions of this approach. We found that a number of respondents preferred optimistic modes to existing access control methods and that interest in optimistic access varied with device type and household characteristics.**

1. Introduction

Consumer Internet of Things (IoT) devices have become widely popular [56], but smart homes pose considerable security and privacy risks, which have yet to be effectively resolved. One class of attacks users are worried about is access by other people in the home [29, 67]. A household may consist of a complex intermingling of device owners and non-owners, residents and visitors, adults and children, and many other categories of users. Because it may be undesirable for *every* person to have access to *any* device, access control is often a required feature for smart homes.

There is a wide variety of designs for smart home access control; some exist only as research prototypes [18, 55, 67], while a small number have been adopted by consumer products [20, 60]. A common assumption is that each individual has their own account, which is not shared. In practice, such assumptions may turn out to be false: a frequent phenomenon is for multiple users to share the same account and password for a single device [33]. Even when access control schemes are designed with usability in mind, users choose to ignore complex configuration options, reporting that they trust their cohabitants and preferring to mediate access through existing interpersonal dynamics, rather than software-based access control methods [67].

The result is somewhat paradoxical. Researchers document privacy violations that are enabled by smart devices [1, 5, 16], and users express a desire for more controls that can help address these [23, 28]. However, they also appear reluctant to adopt systems that would allow for such granular access control. What could be the explanation for this, and how can the situation be improved?

We suggest that a major reason is a cost-benefit analysis: creating accounts and defining access-control policies require a significant time investment, and, for many users, the benefits may be unclear, non-existent, or too far in the future [50]. Further, users may be unwilling to adopt rigid policies due to concerns about unanticipated access needs and unpredicted situations [42]. Many people generally trust others in their household, and those who do may therefore prefer more flexible schemes and arrangements.

We hypothesize that, rather than acting strictly as barriers, these constraints can be leveraged to create new, more practical, user management techniques for smart home devices. We therefore propose a potential solution—optimistic access control for the smart home—and evaluate its acceptability to household users in today's IoT environment.

The idea we evaluate is inspired by literature on "optimistic access control" (OAC) [12, 48]. In lieu of immutable policies, we propose allowing people to obtain the level of access that they believe to be appropriate, while providing sufficient observability so that inappropriate access can be detected by others in the household. The knowledge that others may find out, and that the user will have to face consequences, could be a sufficient deterrent for people not to exceed their authorization without good reason.

Concretely, "optimistic" ideas can be applied to the IoT user experience as follows. When someone new wants to begin using a smart device in a home that they have physical access to, they can do this without obtaining prior authorization, for example, by scanning or entering a code visible on or near the device. At this point, existing users will receive a notification about the new user through their app, which allows them to revoke or otherwise manage the new user's access if they have concerns. This method has the convenience of having a single account and posting its credential publicly, but by assuming each new enrollment is potentially a different user, it allows for better-defined privacy boundaries, for example by compartmentalizing each user's data. Another manifestation of optimistic ideas is to allow users to review data collected by the device—again, without special approval—while ensuring that anyone whose data they review as part of this process will be notified.

Importantly, implementing OAC does not require additional effort or assumptions from IoT device manufacturers. In particular, while the notification and auditing framework relies on apps, existing smart home devices already require apps for managing access control. OAC could therefore be a

drop-in replacement wherever users are currently prompted for passwords or other forms of authentication.

We believe that the optimistic model is a good fit for user management in many smart homes. People already display high levels of interpersonal trust, as evidenced by the popularity of account sharing. But they do have norms and expectations, which can be hard to codify in formal access control policies. OAC frees users from this chore. If misbehavior occurs, they can rely on existing methods of sanctioning it and resolving disputes. (We explore OAC in more detail in §2.2.) However, before proceeding with a system implementation, this intuition must be verified: OAC's design needs to be considered and its acceptability to end users should be tested. This is the focus of our study.

While OAC offers convenience by removing upfront fine-grained configuration and user management, it represents a set of trade-offs surrounding security and privacy. Security is not as strong in OAC as in a system with traditional access control settings because access can be obtained without prior authorization, which can be exploited by people inside and outside the household. (We will explore additional security considerations of OAC in §5.1.) On the other hand, OAC enables user separation and access limits, so it is more secure than everyone sharing the same account. Similarly, OAC may be beneficial to privacy, since access notifications may deter some people from snooping. But the activity notifications themselves can serve as a privacy leak.

Motivated by the above trade-offs, we designed a study to examine the following research questions:

- How do people weigh the security and privacy trade-offs inherent in OAC?
- Which devices might OAC best serve?
- Do people find OAC sufficiently convenient?
- When is OAC a good match for smart homes?

The contribution of our work is answering these research questions. After reviewing the background of the "optimistic" access-control paradigm, we propose a new application for it, centered on the smart home. We then map the design space for this approach and develop several concrete user-experience flows for this scheme. In a series of surveys with 604 participants, we test each access-control domain in a controlled fashion, comparing the effects of device type, household characteristics, and scheme variations. The results show that around 20% of people prefer OAC to existing access-control modes, but the number is almost 40% for certain configurations, such as reviewing data access to sensitive devices like cameras, security systems, and smart locks. Our findings suggest that OAC could be a promising default for certain situations.

2. Related work and background

We survey the literature on access control in the smart home, introduce the background for optimistic access control, and argue for why it is a good fit for smart homes.

2.1. Smart home access control

Access control schemes for computers have been studied for decades [51–53]. Researchers have analyzed the usability of these systems to identify opportunities to increase user adoption [11, 21, 32, 50]. While such studies have influenced the design of access control mechanisms outside academia [22], users in smart home environments display unique behaviors and attitudes [26, 44, 57, 68]. For instance, members of the same household may disagree when setting up or using shared devices [23], while device owners and incidental users can feel tensions over the devices' data gathering and processing practices [9, 17, 40, 66]. Overall, traditional access control schemes do not match users' expectations and needs in the smart home [28].

Access control for smart home devices

There is a rich body of work proposing access control schemes that take into account a variety of contexts and risks [7, 34, 49, 54]; most of these are focused on protecting users from malicious and/or overprivileged devices or apps. Researchers have also investigated real users' threat models and concerns about shared smart home devices. For example, Huang et al. interviewed smart speaker users to understand how they perceive privacy risks [31]. Apthorpe et al. conducted a survey and semi-structured interviews, finding evidence that consumer IoT devices affect interpersonal relationships within multi-occupant households [6]. In parallel, researchers have proposed access control schemes oriented towards smart home contexts. He et al. tested traditional access control techniques in smart home scenarios [28]. The results suggest that those techniques were not very effective for various reasons, such as the interaction modality of many smart home devices not lending itself to easy configuration, definition of access control rules, or authentication. Likewise, Yao et al. ran co-design sessions to try to discover users' privacy preferences and uncovered some potential forms of privacy controls that are vastly different from conventional models, but concluded that they may be inadequate or currently infeasible [65]. Sikder et al. presented an access control mechanism capable of resolving conflicting needs among various household members based on a priority-based technique [55]. Similarly, Dutta et al. designed a system that enforces context-sensitive access control policies [18].

In another study, Zeng and Roesner developed a prototype mobile app to manage various types of access controls in multi-user smart homes [67]. Flexibility and user agency were two of their central design principles, and their prototype supported role-based, location-based, supervisory, and reactive access controls. However, in a user study, the researchers found that most people stopped using the controls, relying instead on social norms, such as mutual trust. Overall, while different smart home access control mechanisms have been designed, most of them have not been adopted in commercial products, among those that do currently exist, few see widespread user adoption [31, 67].

Such results motivate our study. We share the goal of enabling users to achieve appropriate access, but seek to address the complexity by leveraging interpersonal dynamics.

Data review for smart devices and retrospective privacy

As smart home devices are generally shared among various users, researchers have introduced mechanisms that can allow people to audit the usage of their devices and review their data. For example, Zeng and Roesner proposed using activity and discovery notifications to inform users about the usage of their smart home devices [67]. Mennicken et al. developed a calendar-based user interface to facilitate the monitoring of events within smart homes [43]. Castelli et al. proposed a system composed of various visualizations to inform users about their smart home [15]. Additionally, an auditing mechanism for smart home systems based on blockchain technology was proposed by Xue et al. [64].

In addition, retrospective privacy (the study of the correlation between desire to share and the elapsed time since the data sharing) has been studied in different scenarios. Ayalon and Toch demonstrated how users' desire to share posts on social networks decreases over time [8]. Khan et al. examined users' preferences for file retention in cloud storage [36]. They found that many want to remove files that they uploaded to the cloud and then forgot about. This exemplifies the importance of data awareness and management tools that provide users with visibility over their data. Our work extends the literature on retrospective privacy to encompass the smart home by demonstrating potential enforcement mechanisms.

2.2. Optimistic access control

Background. Optimistic access control (OAC) is not a new notion, and its ideas date back decades. The core mantra of "optimistic" security is to *ask for forgiveness, not permission*. Blakley was among the first to suggest that this philosophy can be applied to computer security [12]. Subsequently, Povey elaborated on the concept of optimistic security, also lending it its sanguine name [48]. Later, Peisert and Bishop formalized the notion and applied it to access control specifically [45].

In general, an optimistic access control scheme operates by defaulting to limited permissions but allowing exceptional access at the user's discretion. For example, a physician facing an emergency may choose to exceed their authorization to access the file of someone who is not their assigned patient.

The emergency physician's need to know in an urgent situation is an example of a "break-the-glass" scenario. As its destructive name implies, the scheme only works if the access is noted and scrutinized. If someone exceeds authorization without a good reason, they must face sizeable consequences, which should act as an effective deterrent for anyone considering this decision.

Since its introduction, the idea of optimistic access control has seen limited research and deployment. This is perhaps unsurprising, as there are many situations in which it is clearly inapplicable. For example, it is likely a poor fit for most Internet-connected systems, as the likelihood of tracking down an attacker, and having them face repercussions for their actions, is minimal.

Aspects of OAC can be glimpsed in certain systems, however. The Wi-Fi Easy Connect Specification provides an onboarding method using QR codes or NFC tags [63]. Working groups have proposed bootstrapping transport security on local networks by displaying on-device PIN codes [30]. Researchers of smartphone permissions have suggested "automatic grants" of certain low-risk permissions [19], in concert with effective attribution mechanisms [59], as alternatives to unwanted interrupting warnings.

For smart homes. We observe that optimistic access control may be a good fit for smart home devices, if it is applied to inter-user access management.[1] Users in a household constitute a small circle of people that typically sees limited fluctuations. They have repeated interactions and lasting relationships, which they are motivated to preserve. Consequently, when a household norm is violated and other members find out, the offender is likely to face consequences. Even if those are intangible, such as a loss of trust, they can have significant implications when coming from people who are literally closest to you. Indeed, research suggests that these norms may already be strong enough to substitute for programmatic access control policies [67]. We therefore believe that, in household settings, OAC users will feel major social pressure against violating established norms.

What might those norms be? The difficulty of answering this question is another strength of the OAC model. No two households are entirely alike, so representing subtle differences in expectations using formal policies is exceedingly difficult. OAC may make it possible to side-step this issue. Users could start with limited default access, then adopt additional capabilities as they need them, allowing each household to evolve its own norms. If others consider some access excessive, they can resolve the dispute through interpersonal communication, much like other day-to-day disagreements are handled.

The social resolution of household conflicts represents a key component of the **threat model** of smart-home OAC. The system's subjects are human users with physical access to devices: household members and visitors. Their physical access serves as both a qualification for using OAC as well as an unavoidable property of their role as attackers: they can always tamper with the device directly. However, OAC is designed to protect against *persistent software-based access to devices and their data*. It explicitly allows for the possibility that short-term access may occur, but if it runs counter to the household's norms and expectations, it will be socially sanctioned.

A household's social dynamics are therefore a determining factor for whether OAC will work in it. The power dynamics need not be entirely equal; for example, OAC may work for parent/child relationships. However, the assumptions will break down in situations where the attacker is undeterred by the possibility of being discovered. These may include abusive relationships, one-time visitors, and other circumstances with unequal and/or shifting power dynamics or unexpected events.

1. Another problem in an interconnected smart home is various devices wanting to access each other's and different users' data. This is a different kind of access control problem, which we consider orthogonal.

However, in more favorable conditions, OAC's approach improves usability, since users are not forced to spend time defining access control policies upfront. More people might therefore be willing to adopt distinct user profiles, in a departure from today's default of account sharing. This, in turn, might "unlock" the benefits of separate accounts, such as equity and privacy. When there is a single administrator account, its access may be controlled by one individual, reducing other household members to the status of "passengers users" [37] and limiting their ability to control devices and data about themselves. Separate profiles can help empower all users and increase their independence, if combined with sensible and equitable defaults.

3. Designing an optimistic access policy

We have so far discussed the merits of optimistic access control abstractly, but proceeding with a study of this concept requires defining more specifically how these ideas apply to smart home devices and their interfaces. Next, we present one specific realization of smart home OAC, but observe that it is far from the only one: the abstract idea of optimistic access control—asking for forgiveness rather than permission—may find many different applications in in-home IoT.

Two tasks. We chose to study two different contexts in which optimistic access control may be a good fit: determining (1) who has access to control a device and (2) who can review data on the device. We chose to study these separately because they represent two fundamental facets of the risks surrounding smart home devices. We consider them separable: manufacturers may make different and independent choices about access control for them. We therefore wanted to get independent perspectives on them.

Allowing new users to control a device is often a security or safety issue. We refer to this as the *Onboarding Task* and contrast it with the *Review Task* of choosing who has access to data accumulated by the device, which is more closely associated with privacy issues. These two tasks also allow us to showcase some of the different design decisions that can be made while retaining the overall OAC paradigm.

Defining exceptional access. One of the core principles of OAC is that exceptional access needs to be audited. This naturally raises two questions: what is exceptional access in a smart-home context? And who is doing the auditing? This can vary, and we made slightly different design decisions for each of the two tasks described above.

In the Onboarding Task, we decided that any time a user accessed a device for the first time, this event merited auditing. The auditors would be all household members with existing access to that device. In contrast, in the Review Task, we posited that the person doing the auditing should be the one whose data is being accessed, and that they would be invited to do this each time their data was accessed.

Choosing notification channel. For the purposes of this study, we assumed that each user would install an app associated with their smart device and that, whenever auditing is required, they would receive a notification through this app. A real system might employ additional notification channels and provide fine-grained control over notification frequency.

TABLE 1. SUMMARY OF SURVEYS. * INDICATES THE *in-depth surveys*.

	Task	Variant	Devices	n
0	Pre-survey	No admin pre-approval	*n/a*	20
1	Onboarding	No admin pre-approval	lights, camera	50
2A	Onboarding	Age hierarchy	lights, camera	50
2B	Onboarding	App-based invitation	lights, camera	51
2C	Onboarding	Admin pre-approval	lights, camera	53
3*	Onboarding	Admin pre-approval	lights, thermostat	100
4*	Review	*n/a*	camera, speaker	100
5	Onboarding	Admin pre-approval	TV, media player, speaker, camera, lights, thermostat, outlet, security system, appliances, lock	100
6	Review	*n/a*	TV, media player, speaker, camera, lights, thermostat, outlet, security system, appliances, lock	100

Overall user experience. The complete user experience of OAC might resemble the following. When a new user wants to begin using a smart device in their home, they can enroll by scanning or entering a code visible on or near the device. All existing users will receive a notification about the new user through their apps. Whenever a user chooses to review data collected by the device, anyone whose data they review as part of this process will receive a notification.

This approach shares properties with prior access control implementations. For example, Zeng and Roesner also incorporated activity notifications and notions of reactive access control, but their prototype relied on Role-Based Access Control with per-device configuration [67].

We emphasize that the design details above are one specific case study of optimistic access control. They do not represent the only possible choices, but rather the minimal amount of specifics that we need to evaluate our research questions about people's attitudes towards OAC. We now turn to our strategy for addressing these questions.

4. Methods

The goal of our study was to answer our research questions about the potential promise of optimistic access control by understanding people's perceptions of its usability, security, and privacy. This section describes our approach.

4.1. Study overview

We investigated optimistic access control through a series of surveys (Table 1). We chose this approach over a single

long survey to reduce participant fatigue and data quality issues. This also allowed us to iterate on the design of OAC.

Pre-survey. Prior to our main study, we conducted a pre-survey with 20 participants, testing two ways of explaining the different access control options: using (1) text and (2) visuals in a storyboard format. We did this because we were concerned about the amount of text participants had to read in order to understand the concepts in our study. In spite of our concerns, text-based explanations achieved higher comprehension scores and participant preference ratings, so we used them for the main part of our study.

Iterating on the Onboarding Task. Because there are many valid ways of incorporating optimistic notions into smart home devices, we ran separate surveys ($n = 204$) that tested four distinct variants of the onboarding process, in order to arrive at a design that was most agreeable to respondents. These variants differed primarily in the details of administrative capabilities. The final design of the Onboarding Task is described in §4.3, and our findings about the alternate designs are in §7.5.

Separate surveys for Onboarding and Review. After finalizing the designs of Optimistic Mode, we ran separate *in-depth surveys* (each with $n = 100$) for the two "tasks" introduced in §3: Onboarding and Review. We chose to conduct separate surveys for similar reasons to separating the two tasks. To allow for in-depth follow-up questions, the surveys described so far focused on two smart devices at a time. We selected devices that are (1) sufficiently popular today, (2) currently require—or plausibly need—access control, and (3) have varying levels of risk/sensitivity, to enable comparisons. For the Onboarding Task, these were smart lights and a smart thermostat; for the Review Task, this was a smart camera and a smart speaker.

Comparing multiple devices. The design of the in-depth surveys left open the question of how people feel about OAC for other devices that we had not asked about. To address this gap, we conducted two follow-up *multi-device surveys* (for the Onboarding and Review tasks, each $n = 100$) that solicited preferences about OAC for ten distinct device types.

In all cases, we did not restrict participants to answering only about devices they owned, because this would limit data about less-popular devices and severely reduce cross-device comparisons. Using similar logic, we did not exclude participants who owned no smart devices, since everyone was instructed to "imagine" owning the surveyed device, and we considered these hypotheticals reasonable regardless of which other devices a respondent owned.

4.2. Study flow

Though distinct, each of the six surveys we conducted was structured similarly and proceeded as follows. We began by asking about current device usage and sharing within the respondent's household. We then presented a description of Optimistic Mode as well as two other modes that represented the status quo (see §4.4). After describing the modes, we asked comprehension check questions with an opportunity to correct any mistakes. (Those who got the questions wrong on their second attempt were excluded from the survey.) Next, we asked participants to select their preferred modes for the different device types and to explain their reasoning in open-ended responses. In the in-depth surveys, we also asked about participants' likelihood of adopting a device that used their second- and third-choice mode, as well as to use a 5-point Likert scale to rate the convenience and security or privacy of the modes, in addition to collecting potential concerns about using Optimistic Mode. (A detailed survey instrument is available in Appendix C.)

4.3. Details of Optimistic Mode

In the Onboarding Task, we described "Posted Code mode," in which anyone inside the home can start controlling a device by using an app to enter or scan a code that is displayed on or near the device. The explanation also described two tiers of users: regular users who simply control the device and administrators with access to advanced functionality, such as the ability to revoke access from other users. While anyone can become a regular user by entering the activation code into their app, becoming an administrator requires prior approval from another administrator.

In the Review Task, optimistic notions were expressed in that authorized users (after a one-time approval) could access data stored by the device at any time, but if they accessed any other person's data, that user would receive a notification. The name we used to refer to this was "One-time Approval + Notifications mode."

4.4. Choice of existing modes

In addition to the Optimistic Modes described above, we presented participants with two additional modes in each task. The purpose of these status quo modes was to provide respondents with reference points, so that, rather than evaluating optimistic access control abstractly, which would further be subject to experimenter demand effects, we would instead give participants a choice that would allow them to reveal their preferences. While device manufacturers can choose from a variety of access control options, we distilled them into two modes (in each task) that we felt were representative of the choices most consumers face.

In the Onboarding Task, these were:

- *"One Shared User Account" mode*: everyone shares one account and has the same privileges
- *"Separate User Accounts" mode*: everyone has different accounts and administrators have fine-grained control over privileges

In the Review Task, they were:

- *"One-time approval" mode*: after one-time approval, no one finds out when and what you are reviewing
- *"Request on each access" mode*: permission must be obtained every time a user wants to review data

As a shorthand, the remainder of this paper refers to the four modes above as, respectively, *Single*, *Separate*, *Silent*, and *Request*. The term *Optimistic Mode* was also never exposed to participants, as we deemed it opaque and emotionally valenced. All three task choices were presented

as equals. The full description of all modes, as provided to participants, are in Appendix A.

4.5. Recruitment

We recruited people for our study through the Prolific participant recruitment platform,[2] which screened respondents for being from the United States and age 18 or older. The survey took approximately 15 minutes to complete and offered $4 as compensation. We obtained informed consent from all participants before beginning the survey, and our IRB approved all study procedures.

5. Limitations

5.1. Of optimistic access control

The OAC model encompasses significant security trade-offs. By definition, optimistic access control enables access that other access control schemes would prohibit. This means there is a greater risk of unauthorized actors being able to use a smart device, if only temporarily. However, by design, this applies only to local users with physical access to the home, who can thereby already operate or disable most devices. (Traditional defense mechanisms should continue to be used against network attackers.) We furthermore observe that current deployment practices are already far from perfect, as they are hindered by poor usability and other real-world setbacks. If more people switch from sharing credentials to lightweight access control schemes such as OAC, this may result in a net benefit to privacy and security at scale.

However, as discussed in §2.2, OAC may not be a good fit for all households. By leveraging interpersonal dynamics, it relies on communication and a certain level of trust. Alternate forms of access control may be more appropriate for different types of users, such as domestic workers [10], survivors of intimate partner violence [41], or others with elevated digital safety risks [62] within their home.

Our scheme relies on users being notified of certain actions, so it may be hampered if people turn off their phone's notifications. However, relatively few people disable all notifications [2, 47], and both Android and iOS provide granular control over notifications [4, 24], so a user could allow notifications from an OAC app while denying them for others. Furthermore, research suggests that favorable regimes can be designed for notifications in general [39] and privacy awareness mechanisms in smart homes specifically [58].

A separate consideration is users' auditing behavior: whether they respond quickly enough to notifications—or even pay attention to them at all, due to the potential of fatigue and habituation [3, 61]. This is an important question, though difficult to measure outside real-world deployments, since response times are affected by a variety of factors, including an alert's real-life consequences. We therefore chose to limit our study to people's willingness to adopt OAC, since doing so is a prerequisite for any deployment. By first investigating acceptability, we can identify the best candidates (devices and types of OAC) for future prototypes and associated evaluation of auditing behavior. Nevertheless, existing review behaviors reported by participants in our study (§6.2, below) suggest reasonable engagement (e.g., most households with cameras review footage at least once a month). We recommend a more in-depth exploration of audit behaviors as future work.

2. https://www.prolific.co/

TABLE 2. PARTICIPANT DEMOGRAPHICS ($n = 604$)

Gender	Man	50%
	Woman	46%
	Unknown/other gender identity	4%
Race/Ethnicity	White	66%
	Asian	12%
	Hispanic or Latino	6%
	Black or African American	6%
	Other	10%
Education	No college	15%
	Bachelor's or some college	70%
	Post-secondary	15%

5.2. Of our study

We acknowledge a number of limitations of this paper. First and foremost, we could not study all aspects of optimistic access control as applied to smart homes; to give people concrete choices, we had to narrow down the ideas into specific user experiences, as described in §4. However, other realizations of OAC may be possible and promising; we discuss some of these in §8.3. Another limitation is that our results are based on participants self-reporting their preference between modes, rather than observed behavior in the wild. As with any survey, the statistical power of our data is limited by our sample size, though it was sufficient to show the significance of some statistical effects and to identify additional hypotheses to be tested in future work. While consistent with other survey-based work in our field, our participants may not be fully representative of the population; for example, while the fraction of White people in our study is within 2 percent of the US adult population [35], not every ethnicity may be proportionally represented. Additionally, our study focuses on the United States; while we consider a global perspective very important, for a first study we wanted to focus on one population rather than trying to also compare different cultural and geopolitical contexts. Finally, our results may be subject to experimenter demand effects, though we took steps to mitigate those by giving participants a menu of options, rather than having them express an opinion about only one mode.

6. Participant sample and current behaviors

We begin by summarizing the demographics of our participant sample and their usage of IoT devices.

6.1. Demographics

In total, we recruited 707 people across all our studies. We excluded 95 people who failed comprehension questions after multiple attempts, as well as 8 whose free responses did

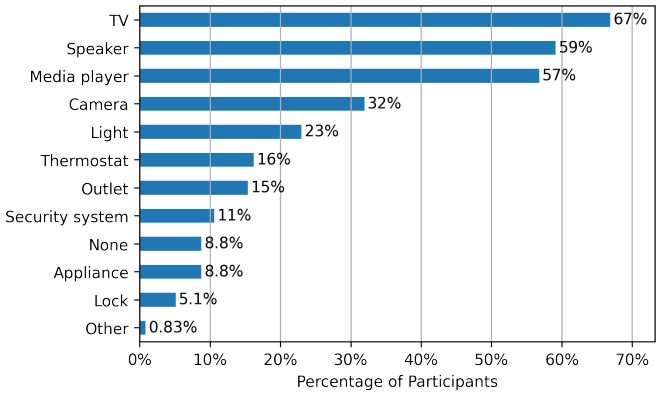

Figure 1. Categories of **devices owned** ($n = 604$)

TABLE 3. **HOW DEVICES ARE SHARED** ($n = 551$)

Share respondent's account	33%
Share other user's account	17%
Share special-purpose account	15%
Each person has separate account	14%
Multiple accounts, some of them shared	9%
Device does not support accounts	7%
Depends on device	4%
Unsure	2%

not address the questions, leaving 604 participants distributed across the different surveys (Table 1).

Table 2 summarizes participant demographics. Respondents ranged in age from 18 to 83 (mean 31, median 29). The sample was approximately balanced by gender, and the majority (close to the proportion of the US adult population [35]) identified as White. As is the norm with online recruitment, our sample skewed towards the educated.

The median household in our study had 3 people, and 31% included children. Among households with children, 53% had one child, and the rest had two or more.

We also asked whether participants had regular visitors who did not reside in their household but might need access to smart home devices. Approximately half (54%) had visitors who needed access (4 people on average). Most commonly, these were friends (51% of those with visitors) or parents/grandparents (46%).

6.2. Current device usage and sharing

Before proposing our scheme and getting people's reactions, we wanted to understand how our participants currently solve the problem of intra-household device sharing.

Device ownership. We started by asking participants which devices they have (Figure 1). More than 90% reported owning some type of smart device: just 8.8% said they had none at all. The median number of devices owned was 3. Smart TVs were most popular, owned by 67% of participants, followed by smart speakers (59%) and TV-attached media players (57%).

TABLE 4. HOW OFTEN OWNERS OF SMART CAMERAS AND SMART SPEAKERS REPORTED REVIEWING HISTORY COLLECTED BY THEIR DEVICES

	Camera ($n = 32$)		**Speaker** ($n = 53$)	
	Self	Others	Self	Others
2+ times a day	4 (12%)	4 (12%)	2 (4%)	0 (0%)
Once a day	5 (16%)	3 (9%)	0 (0%)	0 (0%)
2+ times a week	4 (12%)	9 (28%)	1 (2%)	1 (2%)
Once a week	4 (12%)	4 (12%)	2 (4%)	3 (6%)
2+ times a month	3 (9%)	3 (9%)	0 (0%)	0 (0%)
Once a month	0 (0%)	2 (6%)	6 (11%)	0 (0%)
2+ times a year	4 (12%)	2 (6%)	5 (9%)	4 (8%)
Once a year	4 (12%)	0 (0%)	2 (4%)	1 (2%)
More rarely	2 (6%)	0 (0%)	6 (11%)	4 (8%)
Never	2 (6%)	4 (12%)	22 (42%)	31 (58%)
Unknown	0 (0%)	1 (3%)	0 (0%)	9 (17%)
Don't know how	*n/a*	*n/a*	7 (13%)	*n/a*

Account sharing. We surveyed participants about how they currently share the devices they own (Table 3). We found that a majority (64%) reported sharing a single account between all the smart device users. Only 23% said they had more than one account.

Data review. Since data review is one of the activities our study focuses on, we wanted to know how often people currently engage in this task. (This information also gives us an estimate for an upper bound on how often notifications from our optimistic implementation might occur.) We asked smart speaker and camera owners in the in-depth Review survey about the frequency with which they—or others in their house—reviewed security camera footage or voice assistant interactions (Table 4). Of the 32 participants who owned cameras, the majority reported reviewing footage once a week or less often; they said others review it only slightly more frequently. More respondents owned smart speakers (53 people), but the frequency at which they reviewed their history was lower; more than half reported never reviewing interactions or not knowing how.

7. Results

This section reports our participants' perceptions of optimistic access control for the smart home.

7.1. Access control mode preferences

We first discuss preferences for and against optimistic mode, starting with the multi-device surveys that focus on the acceptability of Optimistic Mode across a wide range of devices, compared with the status quo options.

Few are indifferent. When surveying preferences, we offered respondents an option to express that they did not care about which mode the device had. We found that few people chose this option, indicating that they *do* care. In the Onboarding Task, across all devices, an average of only 9% said they were completely indifferent, ranging from 3% to 17% (Figure 2). P49, for example, explained their choice for smart lights: *"I don't think it makes much of a difference which mode is used because my family members all trust each*

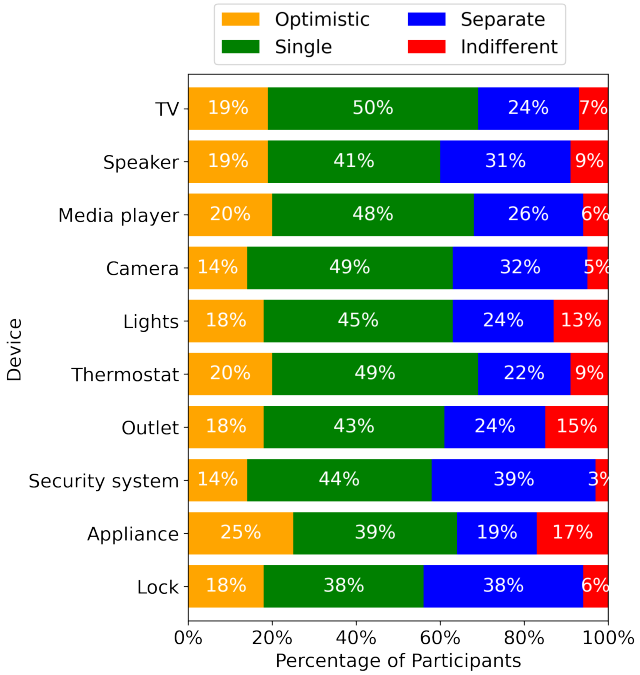

Figure 2. **Onboarding mode preferred** for different device types

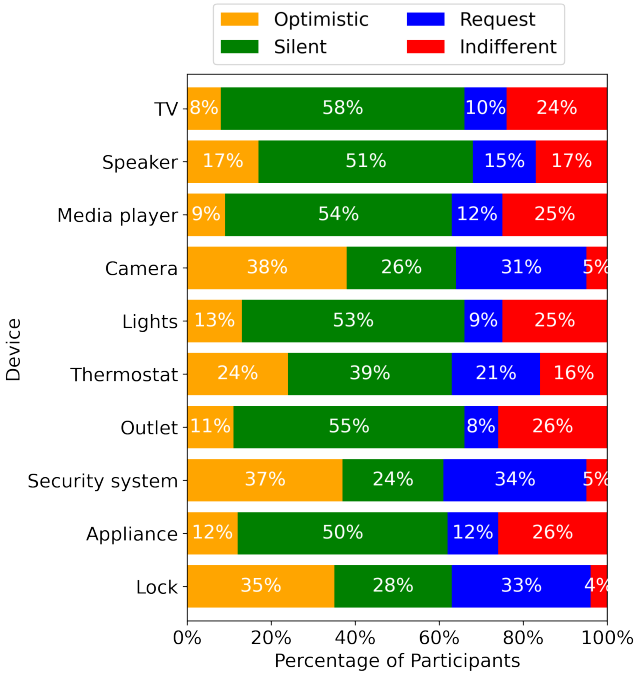

Figure 3. **Review mode preferred** for different device types

other." More people expressed indifference when choosing a Review mode: an average of 17% across all devices, ranging from 4% to 26% (Figure 3).

Shared accounts still preferred for Onboarding. Even with OAC available, having one common account remained the preferred way of sharing devices; across all device types, the plurality chose this method (Figure 2). Nonetheless, a sizeable minority (18% on average) chose Optimistic Mode. It was most favored for smart appliances, where, at 25%, it was the second most popular choice. It was least popular for security systems and cameras, at 14%. We verified that the differences in preferences between the devices were statistically significant using a Chi-Square Goodness of Fit test ($\chi^2(27, N = 100) = 44.6$, $p < 0.05$).

Optimistic popular for Review of sensitive data. In the Review Task, there was greater variability in preferences across devices (Figure 3). For certain types of devices—specifically, for smart cameras, smart locks, and security systems—a plurality of participants favored Optimistic Mode, choosing it over the other access modes. However, it was considerably less popular for other device types, such as smart TVs and media players, where less than 10% of people chose it, preferring "Silent access" mode, in which they were not notified at all about others' activities. On average, Optimistic Mode was chosen a similar number of times as in the previous task: 20%. Once again, the differences between devices were statistically significant ($\chi^2(27, N = 100) = 200.1$, $p < 0.001$).

Replication results show similar trends. Our in-depth surveys presented participants with identical choices of modes, but limited to two device types (§4.1). They therefore serve as verification of the trends seen in the multi-device surveys. The details of these results can be found in Appendix B. The preference patterns were largely consistent with those in the multi-device surveys, though, in the Onboarding Task from the in-depth surveys, Optimistic Mode was more popular for smart lights.

7.2. Effects of household characteristics

To investigate factors that may influence preferences about OAC, for each task, we performed a random-effects[3] logistic regression, with the binary outcome being whether or not the respondent chose Optimistic Mode. (We computed pseudo-R^2 using the Aldrich-Nelson statistic, as it is reported to offer the best performance [25].) Using data from both the in-depth surveys and the multi-device surveys (limited to the devices that appeared in both surveys), we modeled whether each participant chose optimistic mode using the following variables:

1) which device they were choosing for (baseline: thermostat (vs. lights) for Onboarding, speaker (vs. camera) for Review)
2) how they currently share accounts in their household (baseline: separate accounts)
3) number of smart devices they own
4) number of adults in their household
5) number of children under age 10
6) number of children aged 10 or older
7) number of regular visitors who need device access

3. Random effects are necessary due to the inclusion of repeated measures, since we have two choices—one for each device—from every participant.

TABLE 5. REGRESSION FOR ONBOARDING TASK. $n = 200$. PSEUDO-$R^2 = 0.029$

	Odds ratio	Conf. interval	p-value
Device – Lights	2.91	[1.05, 8.12]	0.041*
# visitors	1.18	[1.05, 1.32]	0.007**

TABLE 6. REGRESSION FOR REVIEW TASK. $n = 200$. PSEUDO-$R^2 = 0.13$

	Odds ratio	Conf. interval	p-value
Device – Camera	3.64	[2.01, 6.62]	<0.001***
# adults	1.28	[0.959, 1.72]	0.094
# visitors	1.11	[0.99, 1.24]	0.085

However, most of these factors turned out to not be significant after we performed model selection based on the Akaike Information Criterion [13], which we did to obtain the best model while avoiding overfitting.

Visitor quantity affects Onboarding choice. The regression for the Onboarding Task (Table 5) identified that, for each additional visitor to their household, participants were 18% more likely to choose Optimistic Mode ($\chi^2(1, N = 200) = 7.28$, $p < 0.01$). The model also confirmed the significance of the device type. The odds that a participant chose Optimistic Mode for their smart lights were 2.91 times higher than choosing it for a thermostat ($\chi^2(1, N = 200) = 4.18$, $p < 0.05$).

Device type significant for Review. The regression model for the Review Task (Table 6) likewise identified device type as a significant factor in the choice of access control mode. After controlling for other factors, the odds of a participant choosing Optimistic Mode for a smart camera were 3.64 times higher when compared with smart speakers ($\chi^2(1, N = 200) = 17.99$, $p < 0.001$).

7.3. Security, privacy, and convenience perceptions

We asked participants in the in-depth surveys to rate each of the three modes on a five-point Likert-scale based on its convenience, as well as its security (in the Onboarding Task) and privacy (in the Review Task).

Optimistic Onboarding seen as similar to shared accounts. Participants were generally positive about the security of Optimistic Mode (Figure 4a). While acknowledging that it is not as secure as having separate accounts, nearly half (48%) still rated it as "very" or "somewhat" secure. We verified that the differences between the access control modes were statistically significant using Kruskal-Wallis tests (security: $\chi^2(2, N = 100) = 32$, $p < 0.001$; convenience: $\chi^2(2, N = 100) = 21$, $p < 0.001$).

A core assumption of our study was that Optimistic Mode is convenient. Our results support this hypothesis, with participants rating "Separate accounts" mode as most inconvenient, whereas Optimistic Mode was only slightly less convenient than "Single account" mode (Figure 4b). Based on our specific a priori hypothesis, we followed up the omnibus test with a pairwise Mann-Whitney U test, which

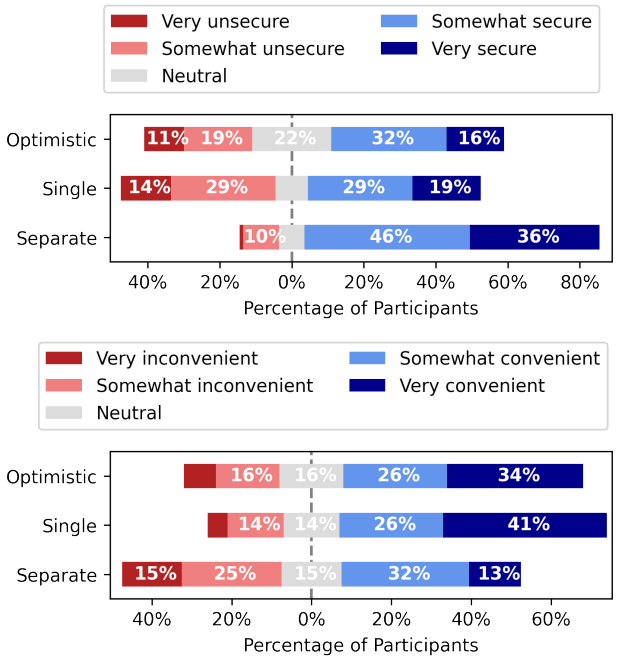

Figure 4. **Onboarding mode perceptions**: participants' answers to the questions
(a) How secure do you think each of the sharing modes is?
(b) How convenient do you think each of the sharing modes is?

failed to find statistically significant differences between the proportions that found these two modes convenient ($Z = 4500$, $p > 0.1$).

Optimistic Review combines privacy and convenience. Perceptions of Optimistic Mode in the Review phase also varied (Figure 5). A large majority (66%) of participants felt that Optimistic Mode did a good job protecting privacy. Most also felt that Optimistic Mode was convenient (60%), especially compared with the nearly three quarters who felt that requesting access for each data review was inconvenient. We verified that the differences in perceptions were statistically significant using Kruskal-Wallis tests (privacy: $\chi^2(2, N = 100) = 67$, $p < 0.001$; convenience: $\chi^2(2, N = 100) = 130$, $p < 0.001$).

7.4. Reasons for choosing modes

For the open-ended responses in our survey, we performed thematic analysis using an inductive approach borrowed from grounded theory [14]. For each question analyzed, two raters read through a subset of responses to identify themes, meeting afterwards to create a combined codebook. The research team conducted affinity diagramming [27] to merge similar codes into higher-level categories. Each rater independently coded every response; the two then jointly resolved differences. We computed interrater reliability using the method of Kupper and Hafner [38].

When inquiring about the preferred access control mode (§7.1), we also asked participants in the in-depth surveys for the reasons behind their choice. We coded these separately for

TABLE 7. COMMON REASONS FOR CHOOSING MODES FOR **ONBOARDING**

	Optimistic		Non-optimistic	
	Lights (n=31)	Thermostat (n=20)	Lights (n=69)	Thermostat (n=80)
More convenient	27 (87%)	6 (30%)	39 (57%)	14 (18%)
Fit their security needs or addressed their security concerns	16 (52%)	15 (75%)	23 (33%)	37 (46%)
Fit their device-sharing behaviors	5 (16%)	14 (70%)	18 (26%)	25 (31%)
Fit their household composition (e.g., number of users, children)	1 (3%)	1 (5%)	17 (25%)	14 (17%)
Due to how they used device (e.g., didn't need to share it with visitors)	5 (16%)	1 (5%)	16 (23%)	15 (19%)
Fit for household's relationships (e.g., help avoid conflicts)	3 (10%)	1 (5%)	9 (13%)	5 (6%)
Trusted people in, or related to, the household with access to the device	0 (0%)	0 (0%)	8 (11%)	2 (3%)
Preferred notification regime	N/A	0 (0%)	N/A	3 (4%)

TABLE 8. COMMON REASONS FOR CHOOSING MODES FOR **REVIEW**

	Optimistic		Non-optimistic	
	Camera (n=29)	Speaker (n=14)	Camera (n=71)	Speaker (n=86)
Liked knowing who has access and who can review data	17 (59%)	5 (36%)	11 (15%)	3 (3.5%)
Liked being informed right away	13 (45%)	2 (14%)	1 (1%)	0 (0%)
Wanted specific mode of approval, such as one-time or every-time	8 (27.5%)	0 (0%)	17 (24%)	25 (29%)
More convenient	7 (24%)	1 (7%)	6 (8.5%)	7 (8%)
Fit household's relationships (e.g., due to trust or power dynamics)	6 (21%)	1 (7%)	0 (0%)	19 (22%)
Appreciated control over who reviews data	5 (17%)	4 (28.5%)	23 (32%)	1 (1%)
Liked level of control (e.g., admin capabilities) provided	5 (17%)	4 (28.5%)	27 (38%)	26 (30%)
Fit their household composition (e.g., number of users, children)	3 (10%)	1 (7%)	17 (24%)	16 (19%)
Concerned about security	2 (7%)	0 (0%)	6 (8.5%)	2 (2%)
Felt that control over review process was unnecessary	2 (7%)	1 (7%)	8 (11%)	22 (26%)
Liked privacy protections	1 (3%)	0 (0%)	5 (7%)	1 (1%)
Due to how they used device (e.g., didn't need to share it with visitors)	1 (3%)	1 (7%)	4 (6%)	21 (24%)
Disliked being informed immediately	1 (3%)	1 (7%)	16 (23%)	13 (15%)
Wanted to prevent device abuse, physical intrusions, or spying	1 (3%)	0 (0%)	3 (4%)	4 (5%)

each pair of smart devices in the Onboarding Task (Table 7)—lights ($IRR = 0.64$) and thermostat ($IRR = 0.49$)—and in the Review Task (Table 8)—cameras ($IRR = 0.54$) and speakers ($IRR = 0.85$). We analyzed each question separately (for a total of four independent codebooks), but here we present the themes grouped by how commonly they were expressed by people who opted for optimistic access control and those who chose a different mode.

Reasons for choosing OAC

People who selected the optimistic access control option generally valued convenience but mentioned its security and privacy advantages as well.

Onboarding is convenient. Participants who chose Optimistic Mode generally did so due to its convenience for themselves and guests: *"I think this is the most flexible option. Created accounts work for people who live in the household, but a visitor isn't going to take the time to create an account just to control a lightbulb"* (P46). They also appreciated the control the mode provided, such as through revocation: *"Anyone there should be able to control the thermostat, but if I don't like what they're doing, I would remove their access"* (P95).

Review raises awareness. Many people liked that the optimistic review mode would bring them awareness of who was accessing their devices and reviewing data: *"I don't mind other people accessing the data but would like to know who does and when they do so if any problems arise then I know who to talk to"* (P77). The ability of notifications to provide instant awareness was also cited as a reason for choosing Optimistic Mode mode: *"Everyone else will get to see what is happening through the cameras, so this mode would be most ideal to me. Plus, I'm really reactive to notifications, so this would be perfect"* (P28). Finally, respondents appreciated the low barrier to access enabled by Optimistic Mode: *"I don't want to have to ask for permission every time I use this thing"* (P28).

Reasons for choosing other modes over OAC

Those who did not choose Optimistic Mode frequently fell on opposite sides of a spectrum: those who wanted maximum control (at the cost of convenience) and those who wanted convenience (with minimal concerns about control).

Wanting more control or convenience in Onboarding. Many respondents described wanting more "control" over the device, such as that provided by traditional role-based access control policies: *"I would choose the 'separate user accounts'*

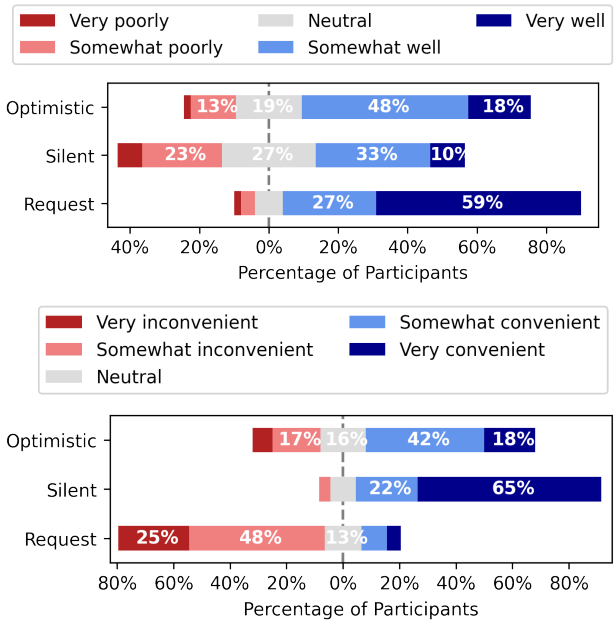

Figure 5. **Review mode perceptions**: participants' answers to the questions (a) How well do you think each of the review modes protects your privacy? (b) How convenient do you think each of the review modes is?

mode because not everyone needs to be in control of the thermostat in my opinion. If they do, the administrator is still in control which is most important" (P15). In contrast, others felt that "Single account" mode was still more convenient: *"I find it more convenient to simply have to give the password of the application to the person who wants to control the lights"* (P53). Finally, some said that they had no intention of sharing certain smart devices with others: *"I chose this mode because I control who has access. I'm a dad... dads just don't let people mess with the thermostat!!"* (P92).

Preferring explicit—or no—approval for Review. Participants opting for non-optimistic modes liked that they afforded exclusive powers to administrators, potentially even as the sole user: *"No one aside from the administrator should be able to freely access the camera as that is a potential for a security flaw"* (P38). Participants often fell in two camps: they either trusted others and so did not want to review any requests, or distrusted them, wanting to review every request: *"I don't think there is any need for any user to be able to have access at any time and I would [be] much more comfortable with others having that access if I approved it first each time"* (P6). For some participants, household composition mattered. Those who lived alone, or only had a partner living with them, felt optimistic mode was a poor fit for their small households: *"I live alone and no one else should need access to the history of my smart speaker"* (P83).

Concerns about Optimistic Mode

We asked participants about potential concerns with Optimistic Mode for both the Onboarding (Table 9, $IRR = 0.66$) and Review Task (Table 10, $IRR = 0.86$). Most concerns about optimistic onboarding focused on perceived security, code-based enrollment, and convenience. With optimistic review, two of the most common concerns were notifications and privacy issues. For both onboarding and review, insufficient control was a central concern.

TABLE 9. COMMON **CONCERNS** EXPRESSED ABOUT **ONBOARDING**

Not secure enough	52 (52%)
Inconvenient or difficult to use	34 (34%)
Disliked code- or scanning-based enrollment	14 (14%)
Unsuitable or unnecessary for certain devices	11 (11%)
Too restrictive	9 (9%)
Consequences of access before pre-approval	6 (6%)

TABLE 10. COMMON **CONCERNS** EXPRESSED ABOUT **REVIEW**

Annoying notifications	38 (38%)
Potential privacy issues	31 (31%)
Insufficient control over access	16 (16%)
Not secure enough	13 (13%)
Inconvenient or difficult to use	9 (9%)
Would not work due to household composition (e.g., the family size was too large)	7 (7%)
Unsuitable or unnecessary for certain devices	5 (5%)
Too much control over access	2 (2%)
Technical requirements	2 (2%)

7.5. Alternate designs of optimistic Onboarding

While we could not explore the full design space for optimistic access control in our study, we tested four alternate designs of Optimistic Mode before arriving at the final formulation of the Onboarding Task. We iterated on our original design because participant feedback suggested we could address some concerns while still staying true to optimistic principles. The procedures for collecting this data were nearly identical to those in the in-depth surveys, except that, among the two devices participants were asked about, the thermostat was replaced with a camera.

We originally envisioned that the onboarding in Optimistic Mode would happen by scanning a QR code; accordingly, Optimistic Mode was initially named *"Scan QR for Setup" mode*. However, approximately a quarter of those surveyed expressed some reservations specifically about QR codes (rather than the access control aspects of the scheme) either for themselves or others, often due to prior frustrations experienced with QR codes. As a result, in the final version of the in-depth survey, we omitted the emphasis on the QR code and stated that the activation code could be scanned or typed manually.

Participants were assigned to one of these mutually exclusive variants:

1) *Admin pre-approval*: As detailed in §4.3, becoming an administrator requires prior approval from another administrator.

TABLE 11. FRACTION OF PARTICIPANTS WHO CHOSE OPTIMISTIC MODE IN EACH OF THE ALTERNATE ONBOARDING DESIGNS

Mode	n	Lights	Camera
Admin pre-approval	53	32%	7.5%
No admin pre-approval	50	18%	2%
Age hierarchy	50	18%	6%
App-based invitation	51	16%	7.8%

2) *No admin pre-approval*: New users can self-identify as regular users *or* administrators; no additional pre-approval is necessary to become an administrator.
3) *Age hierarchy*: New users can self-identify as regular users *or* administrators. However, new users are prevented by policy from revoking permissions of previously existing users, thus precluding the possibility of a "revocation attack" in which an attacker creates a new account and revokes those of existing users before they themselves have a chance to exclude the attacker.
4) *App-based invitation*: This variant was designed to address concerns about both the revocation attack and the publicly posted QR code. Rather than having the QR code posted publicly, an existing user of the smart device has to open their app and show the QR code to the new user, who scans it with their own app. As part of this process, the inviter also chooses the access level of the new user; i.e., they can make them a regular user or an administrator (but the latter only if they themselves are an administrator).

As seen in Table 11, we found the *Admin pre-approval* variant to be most popular, and it became the basis for the final design of the Optimistic Mode in our study.

8. Discussion

Our research offers new insights into user needs and potential solutions for in-home access control.

8.1. Key findings

Our results demonstrate the strengths of optimistic access control and also some of its limitations.

OAC is convenient. Consistent with our expectations, participants perceived the modes that utilized OAC to be approximately as convenient as sharing a single account. This suggests that, if deployed, it may be a promising default option and a usable alternative for people who feel that configuring fine-grained access controls is too burdensome.

OAC improves overall privacy. We further observe that similar proportions of respondents reported having separate accounts for their own smart home devices (23%) and chose "Separate accounts" mode in the survey (e.g., for smart lights, 21%). This suggests that Optimistic Mode may be drawing away users of a single shared account, which would represent a net improvement in their privacy posture.

People are interested in OAC. Most importantly, OAC was the solution of choice for a number of our participants. On average, it was less popular in the Onboarding Task, which looked at how users obtain access to control a device, than in the Review Task, which examined whether people want to know that their data is being accessed. In the latter, Optimistic Mode was chosen by the plurality of participants for several sensitive device types, including security systems and cameras. Due to differences between reported preferences and actual behavior, uptake of OAC may be smaller in realistic conditions than when surveyed. Nonetheless, the concept still appears promising.

Interest in OAC is device- and context-dependent. While Optimistic Mode was moderately popular, it cannot be the solution for everything and everyone. People's interest in optimistic access control is not constant across the board, but rather varies depending on several factors, such as device type and household composition.

Support for OAC is expected to be bounded. What level of interest in optimistic access control is "sufficient?" We believe that no scheme will be perfect for everyone. Some people are satisfied with the status quo: they do not consider the setup process to be a big burden, or they are genuinely satisfied with the security and privacy of a single account. However, there may be others who want more granular controls but are held back by the overhead and rigidity of more complex schemes. OAC could help them achieve their goals, and we saw that there are sufficiently large numbers of people who think it would be a good match for them. We therefore believe that a better way to think about mode popularity is as a question of costs versus benefits: is the cost of implementing this new access method justified by the security that it will bring to the proportion of users that will switch to it from less secure options? In the case of optimistic access control, our results suggest that there are likely to be many users in the US market who might prefer this access-control mode if given the option.

8.2. General lessons for smart-home access control

Our results carry important implications for the design of smart-home access controls broadly, beyond OAC.

Media & security devices most commonly shared. Our data on existing usage of smart devices has important implications for researchers. Most people have multiple smart devices. The most common ones are associated with media consumption: smart TVs, media players, and speakers. The perceived sensitivity of these devices may be low, at least for some users. However, plenty of people use systems with clear security implications, for which at least some access control is strictly required. Among our participant sample, one third had smart cameras, more than 10% had security systems, and one in twenty had a smart lock.

Account sharing should be viewed as default. We also found that 64% of respondents shared one account for all users of their smart devices. This means that the majority is choosing the option that provides the least security and privacy from other household members. We emphasize that this choice may be justified by their threat model, particularly for entertainment devices, and they may be comfortable with the consequences. (Though research suggests that the

concerns may be latent [23].) We believe that the implication for researchers and system designers is that *account sharing is the default* choice made by consumers. Therefore, we should treat it as the baseline when evaluating any proposed access control system and focus heavily on *acceptability*: even if a new system improves security properties, will people who currently share accounts shift to using it?

The majority of participants chose status quo modes, like a single shared account, even when they had the option of choosing OAC. This suggests a strong preference for familiar and easy options, which may affect consumer's choices when presented with other novel access control schemes. This is consistent with established understanding of users' preferences for security systems they are already accustomed to in more general settings [46], even if those preferences lead to less secure behaviors.

More control & transparency needed. Results from the Review Task show demand not just for control over device operations—the traditional subject of access control systems—but also over users' access to each other's data. This is a domain where, currently, smart home users have limited options. More devices should offer data access transparency and controls, with further research needed to determine the specific data types and interfaces.

One-size-fits-all solutions don't work. Demand for auditing capabilities varies with data type; it is higher for devices with more sensitive data, such as security systems and locks, and lower for media players and smart speakers. This shows that people have nuanced views on the sensitivity of different devices, and one-size-fits-all solutions are unlikely to work. For example, a smart camera and smart TV should offer different controls. This reinforces prior work by Zheng et al. [68] and Dutta et al. [18], which showed that presenting different levels of access control in different contexts can better suit users' security and privacy needs.

8.3. Next steps for interpersonal access control

In light of our findings, we envision the following directions as potential next steps in investigating OAC.

Develop context-specific solutions. Our results provide initial indication that OAC's appeal is context-dependent—for example, it may be preferred for certain device types or in specific households—but additional research could help establish more clearly the situations when it would be a good default choice. The smart home environment has the potential to rapidly evolve over a short period of time, and identifying which contexts are associated with what security or privacy preferences is critical in augmenting OAC. Specific areas for investigation include more systematic cataloging of device types and properties, as well as the role of children.

Offer emergency access options. In the design we formulated and presented to participants, "optimistic" ideas were brought front and center, in that users could achieve initial access on their own. An alternate design, which perhaps would align better with original notions of optimistic access control, would be to retain the first step of the administrator assigning everyone roles, but allow users to elevate their privileges only in exceptional circumstances—with the emergency nature emphasized both in explanations and as part of the user experience. We did not test this design, as it is relatively more complicated, but we believe it may appeal to some users and merits further investigation.

Improve user experience pain points. Optimistic access control is a theoretical concept, and translating it into a specific implementation inevitably involves making design decisions that affect the user experience and, therefore, people's perceptions of the underlying idea. However, many of these choices could be substituted for similar ones that might be more appealing to users but retain the core optimistic properties. An example of this that we already incorporated into our study was eliminating the reliance on QR codes, which had proved unpopular with our respondents. We believe there may be other areas for improvement like these. For example, a number of participants in the Review Task expressed concern about the potential volume and frequency of notifications. It may be possible to address this without affecting the privacy benefits of OAC.

Combine OAC with existing access control modalities. In this study, we presented Optimistic Modes as a distinct option from existing modes, such as "Single account" mode. However, interface designers could instead incorporate ideas from OAC into existing systems. For example, if the same account signs in from multiple devices, these could be treated by default as separate profiles, and they could be "upgraded" into separate accounts by an administrator, who could change their access level after the fact.

Differentiate trust levels. OAC can also serve as a foundation for more granular controls. For example, access could be granted optimistically only to a subset of features. Our study began this exploration, showing that people were more comfortable with stringent protections for administrator privileges, but determining optimal ways to differentiate trust levels remains future work.

Integrate with smart speakers. Another promising direction is integrating OAC with voice assistants. For example, assistants could identify new users by their distinct voices and optimistically grant them access; revocation would work by blocking all commands from the specific voice.

Managing accounts and devices among multiple people, especially but not exclusively in households, is and always has been complicated, limited by convenience and effort, and governed in large part by social norms. Technologies that support social norms can be more successful than those that seek to wholly replace social norms with mechanical enforcement. Optimistic access control for the smart home, as formulated in this paper, is one such approach, but we believe that our work is only the beginning of a comprehensive exploration of this subject, and that these ideas can lead to more secure, more private, and more usable smart home experiences for more people.

Acknowledgments

We would like to thank David Wagner for initial conceptual discussions; Omer Akgul, Wentao Guo, and Phoebe Moh for participating in pilots; all of the participants, without whom this research would not have been possible; and Conor Gilsenan for feedback on a draft of the paper.

This paper results from the SPLICE research program, supported by a collaborative award from the National Science Foundation (NSF) SaTC Frontiers program under award number 1955805.

References

[1] A. Acar, H. Fereidooni, T. Abera, A. K. Sikder, M. Miettinen, H. Aksu, M. Conti, A.-R. Sadeghi, and S. Uluagac, "Peek-a-boo: I see your smart home activities, even encrypted!" in *Proc. ACM WISEC*, 2020. [Online]. Available: https://doi.org/10.1145/3395351.3399421

[2] Airship, "Push notifications & mobile engagement: 2021 benchmarks," 2021. [Online]. Available: https://grow.urbanairship.com/rs/313-QPJ-195/images/Push_Notifications_Mobile_Engagement_2021_Benchmarks.pdf

[3] D. Akhawe and A. P. Felt, "Alice in warningland: A large-scale field study of browser security warning effectiveness," in *Proc. USENIX Security*, 2013. [Online]. Available: https://doi.org/10.5555/2534766.2534789

[4] Apple, "Apple advances its privacy leadership with iOS 15, iPadOS 15, macOS Monterey, and watchOS 8," 2021. [Online]. Available: https://www.apple.com/newsroom/2021/06/apple-advances-its-privacy-leadership-with-ios-15-ipados-15-macos-monterey-and-watchos-8/

[5] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, and N. Feamster, "Spying on the smart home: Privacy attacks and defenses on encrypted IoT traffic," *arXiv preprint arXiv:1708.05044*, 2017. [Online]. Available: https://doi.org/10.48550/arXiv.1708.05044

[6] N. Apthorpe, P. Emami-Naeini, A. Mathur, M. Chetty, and N. Feamster, "You, me, and IoT: How internet-connected consumer devices affect interpersonal relationships," *ACM Trans. Internet Things*, vol. 3, no. 4, sep 2022. [Online]. Available: https://doi.org/10.1145/3539737

[7] H. F. Atlam, A. Alenezi, R. J. Walters, G. B. Wills, and J. Daniel, "Developing an adaptive Risk-based access control model for the Internet of Things," in *Proc. iThings*. IEEE, 2017, pp. 655–661. [Online]. Available: https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.103

[8] O. Ayalon and E. Toch, "Retrospective privacy: Managing longitudinal privacy in online social networks," in *Proc. SOUPS*, 2013, pp. 1–13. [Online]. Available: https://doi.org/10.1145/2501604.2501608

[9] J. Bernd, R. Abu-Salma, and A. Frik, "Bystanders' privacy: The perspectives of nannies on smart home surveillance," in *Proc. FOCI*, 2020. [Online]. Available: https://www.usenix.org/conference/foci20/presentation/bernd

[10] J. Bernd, R. Abu-Salma, J. Choy, and A. Frik, "Balancing power dynamics in smart homes: Nannies' perspectives on how cameras reflect and affect relationships," in *Proc. SOUPS*, 2022, pp. 687–706. [Online]. Available: https://www.usenix.org/conference/soups2022/presentation/bernd

[11] E. Bertino, S. Calo, H. Chen, N. Li, T. Li, J. Lobo, I. Molloy, and Q. Wang, "Some usability considerations in access control systems," in *Proc. SOUPS*, 2008. [Online]. Available: https://cups.cs.cmu.edu/soups/2008/USM/bertino.pdf

[12] B. Blakley, "The emperor's old armor," in *Proc. NSPW*, 1996. [Online]. Available: https://doi.org/10.1145/304851.304855

[13] H. Bozdogan, "Model selection and Akaike's Information Criterion (AIC): The general theory and its analytical extensions," *Psychometrika*, vol. 52, no. 3, pp. 345–370, Sep. 1987. [Online]. Available: https://doi.org/10.1007/BF02294361

[14] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, Jan. 2006. [Online]. Available: https://doi.org/10.1191/1478088706qp063oa

[15] N. Castelli, C. Ogonowski, T. Jakobi, M. Stein, G. Stevens, and V. Wulf, "What Happened in my home? An end-user development approach for smart home data visualization," in *Proc. CHI*, 2017. [Online]. Available: https://doi.org/10.1145/3025453.3025485

[16] C. Cobb, M. Surbatovich, A. Kawakami, M. Sharif, L. Bauer, A. Das, and L. Jia, "How risky are real users' IFTTT applets?" in *Proc. SOUPS*, 2020. [Online]. Available: https://www.usenix.org/conference/soups2020/presentation/cobb

[17] C. Cobb, S. Bhagavatula, K. A. Garrett, A. Hoffman, V. Rao, and L. Bauer, ""I would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users," in *Proc. PETS*, 2021. [Online]. Available: https://doi.org/10.2478/popets-2021-0060

[18] S. Dutta, S. S. L. Chukkapalli, M. Sulgekar, S. Krithivasan, P. K. Das, and A. Joshi, "Context sensitive access control in smart home environments," in *Proc. (BigDataSecurity), Proc. HPSC) and Proc. IDS*, 2020. [Online]. Available: https://doi.org/10.1109/BigDataSecurity-HPSC-IDS49724.2020.00018

[19] A. P. Felt, S. Egelman, M. Finifter, D. Akhawe, and D. Wagner, "How to Ask for Permission," in *HotSec*, 2012. [Online]. Available: https://www.usenix.org/conference/hotsec12/workshop-program/presentation/felt

[20] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in *Proc. IEEE S&P*, 2016. [Online]. Available: https://doi.org/10.1109/SP.2016.44

[21] B. Fernandez-Saavedra, R. Alonso-Moreno, A. Mendaza-Ormaza, and R. Sanchez-Reillo, "Usability evaluation of fingerprint based access control systems,"

in *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, 2010, pp. 333–336. [Online]. Available: https://doi.org/10.1109/IIHMSP.2010.88

[22] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed NIST standard for role-based access control," *ACM TISSEC*, vol. 4, no. 3, pp. 224–274, 2001. [Online]. Available: https://doi.org/10.1145/501978.501980

[23] C. Geeng and F. Roesner, "Who's In Control?: Interactions In Multi-User Smart Homes," in *Proc. CHI*, 2019. [Online]. Available: http://doi.org/10.1145/3290605.3300498

[24] Google, "Control notifications on android," 2022. [Online]. Available: https://support.google.com/android/answer/9079661?hl=en

[25] T. M. Hagle and G. E. M. Ii, "Goodness-of-Fit Measures for Probit and Logit," *American Journal of Political Science*, vol. 36, no. 3, p. 762, Aug. 1992. [Online]. Available: https://doi.org/10.2307/2111590

[26] J. Haney, Y. Acar, and S. Furman, ""It's the Company, the Government, You and I": User perceptions of responsibility for smart home privacy and security," in *USENIX Security*, 2021. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/haney

[27] G. Harboe and E. M. Huang, "Real-World Affinity Diagramming Practices: Bridging the Paper-Digital Gap," in *Proc. CHI*, 2015. [Online]. Available: https://doi.org/10.1145/2702123.2702561

[28] W. He, M. Golla, R. Padhi, J. Ofek, M. Dürmuth, E. Fernandes, and B. Ur, "Rethinking access control and authentication for the home internet of things (IoT)," in *Proc. USENIX Security*, 2018. [Online]. Available: https://doi.org/10.5555/3277203.3277223

[29] W. He, V. Zhao, O. Morkved, S. Siddiqui, E. Fernandes, J. Hester, and B. Ur, "SoK: Context sensing for access control in the adversarial home IoT," in *Proc. EuroS&P*, 2021. [Online]. Available: https://doi.org/10.1109/EuroSP51992.2021.00014

[30] HTTPS in Local Network Community Group, "Approaches to Achieving HTTPS in Local Network," Tech. Rep., Sep. 2019. [Online]. Available: https://httpslocal.github.io/proposals/#approach-2

[31] Y. Huang, B. Obada-Obieh, and K. K. Beznosov, "Amazon vs. My brother: How users of shared smart speakers perceive and cope with privacy risks," in *Proc. CHI*, 2020. [Online]. Available: https://doi.org/10.1145/3313831.3376529

[32] P. Inglesant, M. A. Sasse, D. Chadwick, and L. L. Shi, "Expressions of expertness: The virtuous circle of natural language for access control policy specification," in *Proc. SOUPS*, 2008. [Online]. Available: https://doi.org/10.1145/1408664.1408675

[33] W. Jang, A. Chhabra, and A. Prasad, "Enabling multi-user controls in smart home devices," in *Proc. WISP*, 2017. [Online]. Available: https://doi.org/10.1145/3139937.3139941

[34] Y. J. Jia, Q. A. Chen, S. Wang, A. Rahmati, E. Fernandes, Z. M. Mao, and A. Prakash, "ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms," in *Proc. NDSS*, 2017. [Online]. Available: http://doi.org/10.14722/ndss.2017.23051

[35] N. Jones, R. Marks, R. Ramirez, and M. Ríos-Vargas, "2020 Census Illuminates Racial and Ethnic Composition of the Country," Aug. 2021. [Online]. Available: https://www.census.gov/library/stories/2021/08/improved-race-ethnicity-measures-reveal-united-states-population-much-more-multiracial.html

[36] M. T. Khan, M. Hyun, C. Kanich, and B. Ur, "Forgotten but not gone: Identifying the need for longitudinal data management in cloud storage," in *Proc. CHI*, 2018. [Online]. Available: https://doi.org/10.1145/3173574.3174117

[37] V. Koshy, J. S. S. Park, T.-C. Cheng, and K. Karahalios, ""We just use what they give us": Understanding passenger user perspectives in smart homes," in *Proc. CHI*, 2021. [Online]. Available: https://doi.org/10.1145/3411764.3445598

[38] L. L. Kupper and K. B. Hafner, "On Assessing Interrater Agreement for Multiple Attribute Responses," *Biometrics*, vol. 45, no. 3, p. 957, Sep. 1989. [Online]. Available: https://doi.org/10.2307/2531695

[39] T. Li, J. K. Haines, M. F. R. de Eguino, J. I. Hong, and J. Nichols, "Alert Now or Never: Understanding and Predicting Notification Preferences of Smartphone Users," *ACM Transactions on Computer-Human Interaction*, p. 3478868, Feb. 2022. [Online]. Available: https://doi.org/10.1145/3478868

[40] K. Marky, A. Voit, A. Stöver, K. Kunze, S. Schröder, and M. Mühlhäuser, ""I don't know how to protect myself": Understanding privacy perceptions resulting from the presence of bystanders in smart environments," in *Proc. NordiCHI*, 2020. [Online]. Available: https://doi.org/10.1145/3419249.3420164

[41] T. Matthews, K. O'Leary, A. Turner, M. Sleeper, J. P. Woelfer, M. Shelton, C. Manthorne, E. F. Churchill, and S. Consolvo, "Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse," in *Proc. CHI*, 2017. [Online]. Available: https://doi.org/10.1145/3025453.3025875

[42] M. L. Mazurek, P. F. Klemperer, R. Shay, H. Takabi, L. Bauer, and L. F. Cranor, "Exploring reactive access control," in *Proc. CHI*, 2011. [Online]. Available: https://doi.org/10.1145/1978942.1979245

[43] S. Mennicken, D. Kim, and E. M. Huang, "Integrating the smart home into the digital calendar," in *Proc. CHI*, 2016. [Online]. Available: https://doi.org/10.1145/2858036.2858168

[44] P. E. Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. F. Cranor, and N. Sadeh, "Privacy Expectations and Preferences in an IoT World," in *Proc. SOUPS*, 2017. [Online]. Available: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini

[45] S. Peisert and M. Bishop, "Dynamic, flexible, and

optimistic access control," University of California at Davis, Tech. Rep. CSE-2013-76, Mar. 2013. [Online]. Available: https://escholarship.org/uc/item/2rb5352d

[46] S. L. Pfleeger and D. D. Caputo, "Leveraging behavioral science to mitigate cyber security risk," *Computers & Security*, vol. 31, no. 4, pp. 597–611, 2012. [Online]. Available: https://doi.org/10.1016/j.cose.2011.12.010

[47] M. Pielot, A. Vradi, and S. Park, "Dismissed! A detailed exploration of how mobile phone users handle push notifications," in *Proc. MobileHCI*, 2018. [Online]. Available: https://doi.org/10.1145/3229434.3229445

[48] D. Povey, "Optimistic security: A new access control paradigm," in *Proc. NSPW*, 1999. [Online]. Available: https://doi.org/10.1145/335169.335188

[49] A. Rahmati and H. V. Madhyastha, "Context-specific access control: Conforming permissions with user expectations," in *Proc. SPSM*, 2015. [Online]. Available: https://doi.org/10.1145/2808117.2808121

[50] R. W. Reeder, L. Bauer, L. F. Cranor, M. K. Reiter, and K. Vaniea, "More than skin deep: Measuring effects of the underlying model on access-control system usability," in *Proc. CHI*, 2011. [Online]. Available: https://doi.org/10.1145/1978942.1979243

[51] P. Samarati and S. C. de Vimercati, "Access control: Policies, models, and mechanisms," in *International School on Foundations of Security Analysis and Design*. Springer, 2000, pp. 137–196. [Online]. Available: https://doi.org/10.1007/3-540-45608-2_3

[52] R. S. Sandhu, "Role-based access control," in *Advances in Computers*. Elsevier, 1998, vol. 46, pp. 237–286. [Online]. Available: https://doi.org/10.1016/S0065-2458(08)60206-5

[53] R. S. Sandhu and P. Samarati, "Access control: Principle and practice," *IEEE communications magazine*, vol. 32, no. 9, pp. 40–48, 1994. [Online]. Available: https://doi.org/10.1109/35.312842

[54] R. Schuster, V. Shmatikov, and E. Tromer, "Situational access control in the internet of things," in *Proc. ACM CCS*, 2018. [Online]. Available: https://doi.org/10.1145/3243734.3243817

[55] A. K. Sikder, L. Babun, Z. B. Celik, A. Acar, H. Aksu, P. McDaniel, E. Kirda, and A. S. Uluagac, "Kratos: Multi-user multi-device-aware access control system for the smart home," in *Proc. ACM WiSec*, 2020. [Online]. Available: https://doi.org/10.1145/3395351.3399358

[56] Statista, "Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030," 2021. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[57] M. Tabassum, T. Kosiński, A. Frik, N. Malkin, P. Wijesekera, S. Egelman, and H. R. Lipford, "Investigating users' preferences and expectations for always-listening voice assistants," in *Proc. IMWUT*, 2019. [Online]. Available: https://doi.org/10.1145/3369807

[58] P. K. Thakkar, S. He, S. Xu, D. Y. Huang, and Y. Yao, ""It would probably turn into a social faux-pas": Users' and Bystanders' Preferences of Privacy Awareness Mechanisms in Smart Homes," in *Proc. CHI*, 2022. [Online]. Available: https://doi.org/10.1145/3491102.3502137

[59] C. Thompson, M. Johnson, S. Egelman, D. Wagner, and J. King, "When it's better to ask forgiveness than get permission: Attribution mechanisms for smartphone resources," in *Proc. SOUPS*, 2013. [Online]. Available: https://doi.org/10.1145/2501604.2501605

[60] B. Ur, J. Jung, and S. Schechter, "The current state of access control for smart devices in homes," in *Workshop on HUPS*, 2013. [Online]. Available: https://cups.cs.cmu.edu/soups/2013/HUPS/HUPS13-BlaseUR.pdf

[61] A. Vance, J. L. Jenkins, B. B. Anderson, D. K. Bjornn, and C. B. Kirwan, "Tuning Out Security Warnings: A Longitudinal Examination of Habituation Through fMRI, Eye Tracking, and Field Experiments," *MIS Quarterly*, vol. 42, no. 2, pp. 355–380, Feb. 2018. [Online]. Available: https://doi.org/10.25300/MISQ/2018/14124

[62] N. Warford, T. Matthews, K. Yang, O. Akgul, S. Consolvo, P. G. Kelley, N. Malkin, M. L. Mazurek, M. Sleeper, and K. Thomas, "SoK: A Framework for Unifying At-Risk User Research," in *Proc. IEEE S&P*, 2022. [Online]. Available: https://doi.org/10.1109/SP46214.2022.9833643

[63] Wi-Fi Alliance, "Wi-Fi Easy Connect Specification," 2020. [Online]. Available: https://www.wi-fi.org/discover-wi-fi/wi-fi-easy-connect

[64] J. Xue, C. Xu, and Y. Zhang, "Private blockchain-based secure access control for smart home systems," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 12, no. 12, pp. 6057–6078, 2018. [Online]. Available: http://doi.org/10.3837/tiis.2018.12.024

[65] Y. Yao, J. R. Basdeo, S. Kaushik, and Y. Wang, "Defending my castle: A co-design study of privacy mechanisms for smart homes," in *Proc. CHI*, 2019. [Online]. Available: https://doi.org/10.1145/3290605.3300428

[66] Y. Yao, J. R. Basdeo, O. R. Mcdonough, and Y. Wang, "Privacy perceptions and designs of bystanders in smart homes," in *Proc. CSCW*, 2019. [Online]. Available: https://doi.org/10.1145/3359161

[67] E. Zeng and F. Roesner, "Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study," in *Proc. USENIX Security*, 2019. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/zeng

[68] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, "User perceptions of smart home IoT privacy," in *Proc. CSCW*, vol. 2, 2018. [Online]. Available: https://doi.org/10.1145/3274469

Appendix A.
Descriptions of modes offered to participants

A.1. Onboarding Task

Introduction

- To make use of the lights' "smart" functionality (changing colors, setting schedules, etc.), you — and anyone else who wants to control the lights — must install a dedicated smartphone app.
- The person who sets up the device becomes the Administrator. They are in charge of the device.
- *How do additional users get access to the device?* The three "sharing modes" below offer different approaches to answering this question.

"One Shared User Account" mode

- Every member of the household, and any visitor, shares a single account.
- This means that everyone can control the lights, and update settings and schedules, at any time.
- For someone to start controlling the lights, someone — *anyone* — needs to give them the account password.
- The Administrator isn't able to limit what others can do or access: everyone has equal power.
- If the Administrator doesn't like what someone is doing, they can reset the password. The Administrator will have to give everyone the new password, and they will need to sign in again.

"Separate User Accounts" mode

- Every member of the household, and any visitor, is required to have separate accounts.
- This means that, before someone can start using the smart lights, they need to create their own account with an email address and password.
  - Signing up requires performing the following actions on your phone: entering your email address, creating a new password, and verifying the email address.
  - There may be some delay between each of these steps.
- After someone creates an account, the Administrator has to explicitly grant them permission to control the lights.
  - To do so, the Administrator needs to navigate in the app, find their email address and select the appropriate access level. This may take a minute or so.
- The Administrator can decide on different levels of access for each person.
  - For example, some people may be allowed to adjust the lights but not change any schedules.
  - The Administrator, and anyone they delegate administrative abilities to, can also revoke or expire access, for example, after it's no longer needed.

"Posted Code" mode

- Every member of the household, and any visitor, can begin to control the lights by typing in, or scanning, an activation code displayed on (or near) the smart lights.
  - They'll also need to enter their name.
- As soon as they do this, they can begin controlling the device. This includes basic functionality, like turning it on and off, but *not* advanced features like changing settings, setting schedules, or managing users.
  - To get access to the advanced (Administrator) features, a user will need to be approved by an existing Administrator.
- Administrators can control advanced features like settings & schedules and also manage (approve or remove) other users.
  - If an Administrator disapproves of someone joining, they can remove them from the device.
  - The removed user won't be able to regain control, even if they put in the activation code again.
- All users are immediately notified (through the app, or by email or SMS if they prefer) when another user joins, what their name is, and whether they are an Administrator or a regular user.

A.2. Review Task

Introduction

- Access to the smart camera is managed through the *"Smart Home App."*
  - For the purposes of this study, please assume that everyone who needs access has *already installed* the Smart Home App.
  - Likewise, please assume that every user has a *separate account* on the Smart Home App that they already set up.
- Who gets to access video **footage recorded by the camera**? The three "**review modes**" below offer different approaches to answering this question.

"One-time approval" mode

- Only authorized users are able to review footage.
  - The device's Administrator can authorize other users to review footage.
- Once they've been authorized, users can review footage **at any time, whenever they want.**

- **No other user will find out** if and when a user reviews footage, even the device's Administrator.

"Request on each access" mode

- Only authorized users are able to review footage.
  - The device's Administrator can authorize other users to review footage.
- Users need to **request authorization every time** they want to review footage.
- Because of the authorization process, the **Administrator will know when and what** the user is accessing.
  - But **users who aren't the Administrator won't find out.**

"One-time approval + notifications" mode

- Only authorized users are able to review footage.
  - The device's Administrator can authorize other users to review footage.
- Once they've been authorized, users can review footage **at any time, whenever they want.**
- Users **receive notifications if footage with them is reviewed** by someone else.
  - In other words, if another user reviews footage and you appear in it, you will receive a notification about this.
    - For example, you might get a notification that says: "You were captured on your security camera yesterday at 9 AM. User __ has just reviewed that activity."
  - This notification will be shown to all Smart Home App users, regardless of who reviews them, even if it is the device's Administrator.
    - People who are *not* Smart Home App users (for example, household members who don't have accounts, visitors, passers-by, or burglars) will *not* get notifications or find out that footage with them has been reviewed.

Appendix B. Mode preferences from in-depth surveys

In §7.1, we report participants' preferences between the Optimistic Mode and the status quo options as expressed in the multi-device surveys. This section reports the analogous results from the *in-depth surveys*, which focused on two devices at a time.

In the Onboarding Task (Figure 6), for smart lights, more people (31%) chose Optimistic Mode over fully separate accounts (21%). It was less popular for thermostats, at 20%. Most respondents were consistent in their choice between devices: 58% chose the same Onboarding mode for both devices. (The respective number for Review was 59%.)

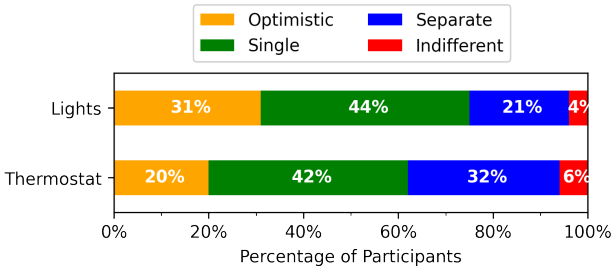

Figure 6. **Onboarding mode preferred** by participants for smart lights and smart thermostats

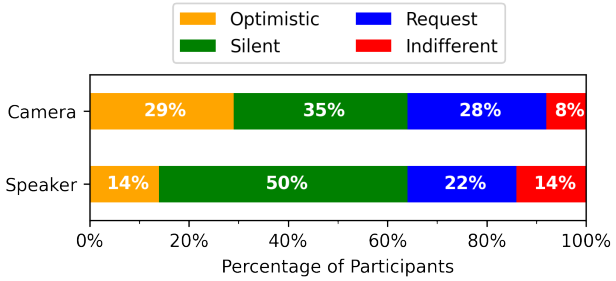

Figure 7. **Review mode preferred** by participants for smart cameras and smart speakers

In the Review Task (Figure 7), for smart cameras, Optimistic Mode was relatively popular, with 29% opting for it. In contrast, only 14% chose Optimistic Mode for smart speakers. In both cases, the plurality of participants preferred not being notified about data access (35% and 50% for cameras and speakers, respectively).

Appendix C. Survey instrument

Due to page limits, the survey instrument is hosted at https://osf.io/f54u2?view_only=034075107 29a467aa562489ee6426020.