Privacy Equilibrium: Balancing Privacy Needs in Dynamic Multi-User Augmented Reality Scenarios

Shwetha Rajaram
University of Michigan
Ann Arbor, MI, USA
shwethar@umich.edu

Jiasi Chen
University of Michigan
Ann Arbor, MI, USA
jiasi@umich.edu

Michael Nebeling
University of Michigan
Ann Arbor, MI, USA
nebeling@umich.edu

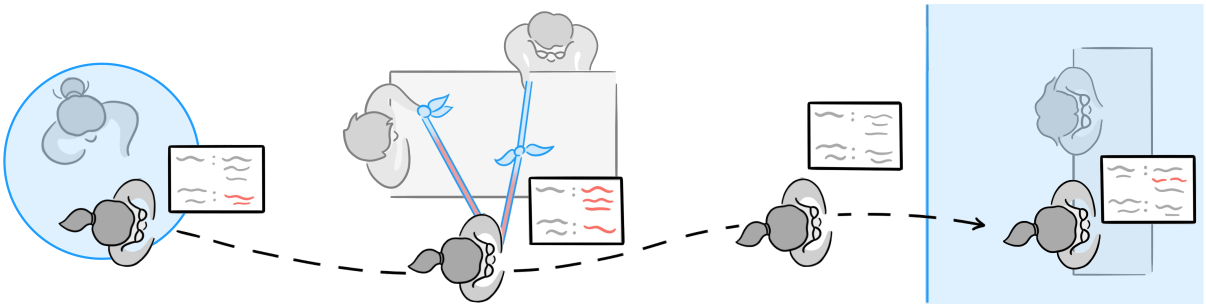


Figure 1: Augmented reality glasses pose privacy risks for co-located individuals, but today, their use in public spaces is governed solely by the wearer. Our work explores how to facilitate multi-user negotiations of AR sensing capabilities, formulating this process as an optimization approach to maintain core AR functionality while achieving a balance, or Equilibrium, with privacy.

Abstract

As augmented reality (AR) glasses become more widely used in public settings, a key challenge is meeting the privacy needs of multiple AR users and bystanders in a fine-grained manner. To enable this, we present a conceptual framework for *Privacy Equilibrium*–balancing user experience (UX) and privacy between all individuals in a shared space. The framework applies constrained optimization to compute AR sensing policies that grant or restrict permissions to maximize UX while minimizing privacy risks (e.g., capturing bystanders or sensitive environmental data). We instantiate this framework in a simulation and analysis toolkit to holistically evaluate different optimization strategies and visualize tradeoffs between UX and privacy. Through application scenarios, we demonstrate the flexibility of our optimization approach to minimize these tradeoffs across conflicting user needs and privacy preferences. Walkthrough evaluations with AR and security & privacy researchers highlight the potential of our framework and toolkit to inform future privacy-mediating techniques for AR.

CCS Concepts

• **Human-centered computing** → **Mixed / augmented reality**; • **Security and privacy** → *Usability in security and privacy.*

Keywords

adaptive AR interfaces, usable privacy, simulation

UIST '25, Busan, Republic of Korea

ACM ISBN 979-8-4007-2037-6/25/09
https://doi.org/10.1145/3746059.3747783

ACM Reference Format:
Shwetha Rajaram, Jiasi Chen, and Michael Nebeling. 2025. Privacy Equilibrium: Balancing Privacy Needs in Dynamic Multi-User Augmented Reality Scenarios. In *The 38th Annual ACM Symposium on User Interface Software and Technology (UIST '25), September 28–October 01, 2025, Busan, Republic of Korea.* ACM, New York, NY, USA, 24 pages. https://doi.org/10.1145/3746059.3747783

1 Introduction

Consider a person with vision impairments navigating a hospital with AR smartglasses that provide scene descriptions and assist with wayfinding [8, 19]. As they walk, their AR glasses narrate ongoing events, such as family members visiting patients and doctors running to their next appointments, some of whom are using AR themselves. In this dynamic and sensitive context, how, if at all, should the AR system adapt to protect the privacy of others around? Should it reroute the user to avoid bystanders? Could it describe the scene with less specificity, or would that hinder the user's ability to navigate safely? And, how can the user safeguard their own privacy while navigating among other AR users?

As always-on AR devices become more common in everyday settings, scenarios like these will increasingly arise, where sensing capabilities essential for AR functionality require tradeoffs in privacy for users in a shared space. Studies with early adopters of AR technologies highlight concerns with AR systems' potential to infer their identity, health conditions, behavioral patterns, or sensitive details about their surroundings [1, 12, 17] – all of which are risks that bystanders also face due to how AR devices capture and process user input and the environment [13, 16, 30]. To enable both AR users and non-users to meet their privacy needs in shared spaces, the HCI and security & privacy (S&P) communities envision access control techniques that regulate the use of AR sensing capabilities to minimize the capture and exposure of sensitive data. Proposals range from world-driven broadcasting of sensing policies that apply to all users in a space [39], to user-driven specification of permissions to follow contextual rules [21, 24, 38] or to achieve acceptable tradeoffs between privacy and functionality [2].

However, we identify two key shortcomings in this landscape of privacy-mediating techniques for AR. First, sensing policies are governed by a single entity–either individual users or space owners–leaving other people in the environment subject to this entity's goals and decisions. Our motivating scenario demonstrates one such tension: the use of visual assistive technologies poses privacy risks for bystanders, yet any hospital-wide restrictions on environmental sensing could threaten user safety. This leads to the second challenge: existing techniques for controlling sensing access can incur different tradeoffs between AR user experience and privacy, but are rarely assessed comparatively, limiting our understanding of which approaches best reconcile competing user needs.

Developing more robust privacy-mediating techniques for AR requires *(1)* accounting for the diverse, and sometimes conflicting, needs of multiple individuals in shared, dynamic environments, and *(2)* analyzing the tradeoffs of different approaches in relation to each other to identify which of them best meet the collective UX and privacy needs of users. Our work offers two related contributions. First, we introduce a **conceptual framework for balancing user experience and privacy needs among multiple AR users and bystanders through facilitating system-driven *negotiations* of sensing capabilities.** The framework applies constrained optimization to compute AR sensing policies, granting access to application-critical sensing requirements while satisfying the privacy preferences of co-located individuals–a state we refer to as *Privacy Equilibrium.* Second, we **instantiate the framework in a simulation and analysis toolkit** designed to enable AR and S&P researchers to holistically explore privacy-mediating techniques for future usage scenarios. The toolkit supports modeling multi-user interactions and sensing negotiations based on our optimization approach, and comparing tradeoffs between UX and privacy through a visualization dashboard.

To assess the effectiveness of our optimization approach for balancing diverse user needs, we first conducted an application-driven evaluation [27], using our toolkit to compute and analyze sensing negotiation strategies for our motivating hospital scenario and multi-user interactions in an office setting. To further validate the framework dimensions and their instantiation within the toolkit, we conducted walkthrough evaluations with 8 researchers working at the intersection of AR and S&P. They found our optimization approach offered greater flexibility than prior work, reaching acceptable compromises among competing user goals and giving all users a say in the negotiation. Informed by discussions with these researchers, we discuss improvements to our framework to capture user-aligned perceptions of privacy and future work to bridge the gap to implementing such AR privacy-mediating techniques.

2 Background & Related Work

In this section, we review prior work on privacy concerns arising from the use of AR in public, multi-user settings, along with privacy-mediating techniques that aim to mitigate these risks by adjusting AR sensing capabilities across contexts.

2.1 Privacy Concerns with AR Usage in Shared Physical Settings

Novel AR sensing capabilities that enable natural input techniques (e.g., gesture and speech recognition) and context-aware interactions with users' environments (e.g., spatial mapping, object detection) can raise a variety of privacy concerns [12, 37]. Several recent studies have investigated how early adopters perceive these risks [1, 3, 17], with common concerns around inference of physiological and biometric traits, identity, personal characteristics (e.g., gender, race), mental state, and environmental cues that may reveal location or activity patterns.

Because AR sensing techniques are designed to perceive and augment users' surrounding environments, these risks can extend to others who are co-located in the space. Surveys and user studies with potential bystanders of AR highlight two key reasons that these risks could be exacerbated [4, 10, 13, 16, 30]. First, bystanders are often unaware of passive sensing and lack meaningful mechanisms to provide consent or exert control over their data, which is likely to worsen as AR glasses become more lightweight and subtle [13]. Second, when bystanders are aware, their discomfort increases due to uncertainty about how AR applications use their data, especially when it is retained for later use (e.g., stored spatial maps) or processed by third parties (e.g., for training or improving tracking algorithms).

While AR users often wish to respect bystander privacy, they currently have limited means to notify bystanders or obtain their consent [6]. Their current coping strategies include pausing AR tasks or relocating to empty spaces to avoid bystanders, requiring significant manual effort and limiting the practicality of AR use [17].

2.2 Privacy-Mediating Techniques for AR Users and Bystanders

As AR devices are increasingly used in public settings, the HCI and security & privacy communities are actively investigating technical approaches to mitigate associated privacy risks. Prior work developed a broad range of privacy-enhancing technologies (PETs) such as obfuscation techniques to limit AR apps' access to raw sensor streams [11, 20], differential privacy to obscure motion data [29], and interaction techniques that disclose less detail to bystanders and distributed collaborators [33], such as silent speech [45]. Rajaram et al. establish a design space of such techniques for adapting AR interfaces to meet users' privacy needs while maintaining core AR functionality [34]. Prior work also contributes design and development tools to guide the implementation of PETs for AR [25, 35].

In particular, **our work builds on AR access control frameworks that operate at the application permissions level**. These frameworks aim to prevent privacy risks caused by the capture and exposure of environmental data in shared spaces by restricting AR applications' access to sensing capabilities in privacy-sensitive contexts. Examples include:

(1) **World-Driven Access Control** [39] which enforces sensing policies for all users in a space (e.g., universally restricting video capture near sensitive areas such as bathrooms);
(2) **User-driven permission frameworks**, which allow users to dynamically configure AR applications' sensing access based on contextual rules [21, 24, 38] (e.g., permitting object detection

only in certain locations or only when app features requiring this capability are activated), or to achieve desired levels of privacy–functionality tradeoffs [2] (e.g., allowing sound detection but not speech recognition);

(3) **Peer-driven permission frameworks** to mitigate interpersonal privacy concerns in multi-user AR scenarios [10, 26, 32], defining collaborators' access to view, modify, and share sensitive physical or virtual content [9, 36, 40, 42, 46].

However, a key limitation of these frameworks is their inflexibility in accommodating multiple individuals' varying AR usage and privacy needs, as data access is determined by a single entity: individual users in user- and peer-driven frameworks, or space managers in World-Driven Access Control. While a single governing entity may be desirable in privacy-sensitive contexts, some situations require a more nuanced consideration of individuals' needs (e.g., our motivating scenario, where a low vision user's safety should take precedence when using assistive technologies, even if bystander privacy is affected).

To meet the UX and privacy needs of multiple individuals in shared spaces, we re-envision AR access control as a negotiation of sensing capabilities, leveraging optimization to dynamically grant or restrict permissions rather than a static rule-based approach.

3 Research Approach

Our research process started with drafting an initial *Privacy Equilibrium* framework that characterizes multi-user AR sensing negotiations (Sec. 4) through two key dimensions: the scope of users involved and optimization strategies that grant sensing permissions to prioritize different objectives or stakeholders. This framework not only encompasses the new optimization-based access control strategy we propose in this work, but can also be used to express existing approaches from prior work (Sec. 2.2), e.g., World-Driven Access Control [39].

Then, we developed a toolkit to simulate multi-user AR scenarios across physical environments and analyze the impact of various sensing negotiation strategies on users' UX and privacy (Sec. 5). The toolkit serves two primary goals. First, it supported our research process by enabling us to refine and assess the implementation feasibility of the framework, through formalizing key concepts as optimization problems. Second, it provides a research & development platform for AR and S&P researchers and developers to holistically explore sensing requirements and compare access control techniques for future AR usage scenarios. We use simulation to enable this exploration, drawing on its established role in HCI as a method for investigating the feasibility and sociotechnical implications of emerging technologies, particularly when user testing is constrained by limitations of real-world infrastructure or potential safety risks [28, 41]. Recent work in the UIST community leveraged simulation to evaluate UI adaptation techniques across diverse user preferences [22], model human body motion [18], and assess to what extent LLM-driven agents can mimic social behavior [31].

We evaluated the expressiveness of the framework and toolkit in bridging the gap between multiple individuals' diverse needs in two steps. First, we conducted experiments around two application scenarios where AR use poses significant privacy risks, demonstrating that our optimization approach effectively balances UX and privacy across individuals (Sec. 6). Finally, we conducted walkthrough evaluations with S&P experts to inform improvements to the framework's instantiation within our toolkit (Sec. 7).

4 Privacy Equilibrium Framework

In this section, we present our conceptual framework for establishing a *Privacy Equilibrium*–a balance between the user experience and privacy needs of all AR users and non-users in a space. In line with existing access control approaches (Sec. 2.2), we consider how to achieve this balance by adjusting which AR sensing capabilities a given group of users are permitted to use. This poses a major challenge for dynamic multi-user AR settings, as it requires bridging the gap between heterogeneous AR devices, AR applications, and a range of users' privacy preferences. We show that by **re-envisioning AR access control as a *negotiation* of sensing capabilities between multiple individuals and modeling negotiations via constrained optimization**, our framework can generate sensing policy configurations that flexibly accommodate varying user requirements.

We start by discussing our Design Goals (Sec. 4.1) and detailing the process for sensing capability negotiations (Sec. 4.2). Then, we introduce two dimensions that characterize negotiations: the scope of participating users (Sec. 4.3) and optimization strategies used to negotiate permissions across users to achieve UX- and privacy-oriented objectives (Sec. 4.4). Finally, we explain how we formulated optimization problems around these dimensions (Sec. 4.5-4.6).

4.1 Design Goals

Inspired by our review of related work, we defined three key design goals for our framework:

(1) **Modeling AR sensing capabilities:** We aimed to allow flexible representations of permission models for future AR glasses that offer fine-grained control over individual sensing capabilities (e.g., switching from cloud to local processing for speech recognition, rather than restricting speech input altogether).

(2) **Modeling privacy needs of multiple AR users and non-users:** Our second design goal was accounting for the needs of everyone who could face bystander privacy risks in a given physical environment, including both AR users and non-users. In doing so, our work bridges separate research streams on interpersonal privacy considerations for multi-user AR [32, 40] and bystanders of AR usage [10, 13].

(3) **Modeling tradeoffs between UX & privacy:** Finally, despite Privacy by Design [7] being a core goal in the usable privacy community, today's landscape of privacy-preserving techniques for AR can come at the cost of usability and functionality, and vice versa [2, 34]. In line with prior work on AR and IoT systems [2, 14, 49], we aimed to assess the tradeoffs that sensing restrictions impose on both AR users and bystanders.

4.2 Negotiation of AR Sensing Capabilities

At the core of our framework is a process we refer to as a **negotiation of AR sensing capabilities, which determines how to adjust an application's sensing permissions to align with the interpersonal privacy preferences of co-located individuals.** This requires two types of input:

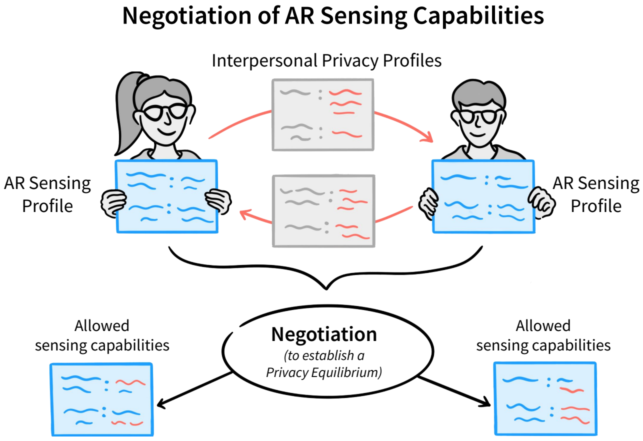

Negotiation of AR Sensing Capabilities
Interpersonal Privacy Profiles
AR Sensing Profile
AR Sensing Profile
Negotiation
(to establish a Privacy Equilibrium)
Allowed sensing capabilities
Allowed sensing capabilities

Figure 2: Negotiation of Sensing Capabilities

(1) An **AR Sensing Profile**, which specifies the set of sensing capabilities an AR application requires to achieve the optimal user experience. As with traditional permission models, developers would specify these requirements, and users can grant or revoke access based on their individual needs and privacy preferences. For example, a Navigation app may just need location access to provide directions, but also require live spatial mapping to help a low-vision user navigate around obstacles in real time.
(2) An **Interpersonal Privacy Profile**, which specifies the set of sensing capabilities each user is comfortable with others around them utilizing. For example, someone may object to others performing spatial mapping in their home. Our current framework assumes users will define these profiles manually or choose a predefined profile aligned with a privacy persona, such as a highly risk-averse *Privacy Fundamentalist* or a *Privacy Unconcerned* individual [15]. We also envision mechanisms for AR non-users to express their privacy preferences (e.g., a QR code-linked survey upon entering a space).

Figure 2 illustrates a sensing negotiation process for two AR users, where each user's AR Sensing Profile is adjusted to align with other co-located individuals' Interpersonal Privacy Profiles, resulting in an allowed set of sensing capabilities for each user. While out of scope for our framework, we envision that AR interfaces could adapt their interaction techniques in response to negotiations to preserve functionality as much as possible [34]. For example, if speech recognition were restricted, an AR interface could rely on alternative input methods such as typing or gestures [33].

While Fig. 2 shows a simple case, we can facilitate negotiations to produce many alternative solutions, with outcomes varying based on the users involved and how their conflicting preferences are resolved. For example, we could prioritize granting permissions for AR users with accessibility or safety needs, or restricting permissions in sensitive physical contexts.

To capture these aspects, our framework characterizes negotiations through two dimensions: *Equilibrium Scope*–who participates in the negotiation process–and *Optimization Strategies*–approaches to guide negotiations toward a particular Equilibrium point, each representing a distinct tradeoff between UX and privacy for users within the scope. Our framework also includes metrics for approximating these tradeoffs, allowing comparison of solution points along a curve, known as the Pareto Frontier (Fig. 5), to identify optimal solutions. We describe each concept in turn.

4.3 Equilibrium Scope: Who Is Involved

First, our framework defines the Equilibrium Scope dimension, which determines which users are involved in the negotiation process (Fig. 3). Based on our literature survey, we consider three approaches:

- **Space-Wide:** All individuals in the physical environment–defined by natural boundaries like walls or doors–participate in the negotiation. This results in a sensing policy that grants or restricts specific AR sensing capabilities across the entire space or within spatial subsets, such as rooms or hallways. This approach is ideal for capturing space-based social norms around privacy (e.g., adopting a more restrictive policy in a privacy-sensitive hospital).
- **Zone-Wide:** Each person is allocated a portion of the physical space (a zone), and negotiations occur between users in overlapping zones. These zones could be *user-anchored*, traveling with users as they move within the space, or *space-anchored* (e.g., a fixed sensing zone around one's office desk). The latter approach is useful when marking temporary personal areas (e.g., when working in a public cafe).
- **Peer-to-Peer:** Negotiations take place between pairs of individuals. When based solely on proximity, Peer-to-Peer produces similar sensing policies to Zone-Wide in two-user scenarios, but enables more granular policies for chained configurations of three or more users. For example, in Zone-Wide, a privacy-conscious user may influence all users in overlapping zones, whereas in Peer-to-Peer, their preferences primarily affect the user within closest proximity. While not currently modeled in our optimization formulation (Sec. 4.6), Peer-to-Peer policies could also account for user roles (e.g., applying more permissive rules for friends and family, and stricter ones for strangers).

Respective examples of each from the literature include World-Driven Access Control [39] for Space-Wide, zone-based sharing for collaborative AR experiences [40], and peer-to-peer content viewing policies for public digital displays [43].

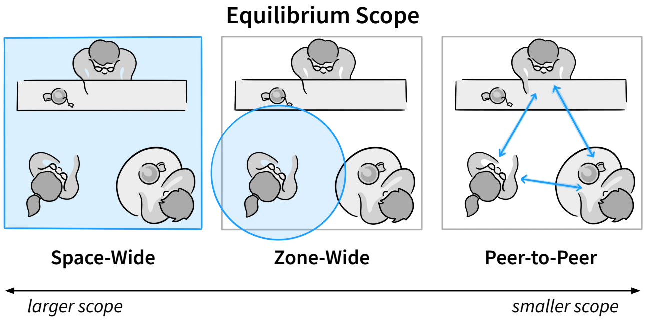


Figure 3: Equilibrium Scope

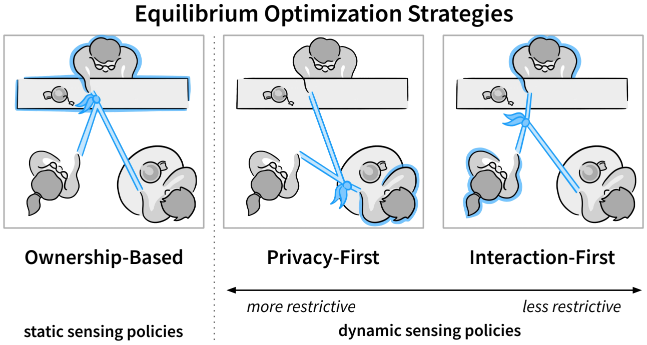


Figure 4: Equilibrium Optimization Strategies

4.4 Equilibrium Optimization Strategies: Promoting Specific Objectives

While our framework's first dimension concerns the Equilibrium *scope*, the second concerns the Equilibrium *point*: whether the goal is for all users to make similar compromises in UX and privacy, or to reach a more nuanced balance point that prioritizes specific values or stakeholders. For example, in sensitive contexts like hospitals, more restrictive sensing policies may be favored to safeguard visitors' privacy. Other scenarios may warrant prioritizing UX, especially when users have a critical need to use AR (e.g., for accessibility) or where appropriate privacy measures are in place (e.g., an experimental setting with informed participant consent).

We define three strategies for optimizing sensing negotiations to promote these different goals (Fig. 4). The Ownership-Based strategy reflects access control models from prior work, where a single entity determines sensing policies (Sec. 2.2). We propose Privacy-First and Interaction-First optimization as new strategies to bridge the gap between multiple users' requirements.

- **Ownership-Based:** This strategy's objective is adhering to a sensing policy defined by a designated space owner, who sets the privacy and social norms for a physical space and determines the AR sensing capabilities permitted within it. For example, policies could be dictated by a coffee shop manager or teacher under the Space-Wide scope, or by individual users who "own" portions of the surrounding space using the Zone-Wide scope.
- **Privacy-First:** Negotiations are optimized to uphold individuals' Interpersonal Privacy Profiles, resulting in a more restrictive set of allowed AR sensing capabilities. In other words, the objective is to maximize overall user satisfaction in terms of privacy.
- **Interaction-First:** This strategy grants access to sensing capabilities in a more permissive manner, to prioritize the user experience of AR users based on their AR Sensing Profiles. Conversely to Privacy-First, the optimization objective for Interaction-First is maximizing overall user satisfaction in terms of UX.

We note that the Privacy-First and Interaction-First objectives guide negotiations toward two extremes–prioritizing either the protection of interpersonal privacy or the granting of AR sensing capabilities. To achieve Equilibrium points that reflect more balanced tradeoffs, we can optimize for one objective while treating the other as a constraint, which we will demonstrate in Section 4.6. This approach requires computational metrics to assess tradeoffs between objectives, which we describe next.

4.5 Equilibrium Scores: Assessing Tradeoffs

Finally, our framework introduces two Equilibrium Scores, which quantify to what extent users' AR Sensing and Interpersonal Privacy Profiles are upheld before and after sensing negotiations (Fig. 5):

(1) **Permission Satisfaction Score:** The weighted sum of each user's required AR sensing capabilities (as specified in their AR Sensing Profiles) that they are allowed to use.
(2) **Privacy Satisfaction Score:** The weighted sum of each user's privacy preferences (as specified in their Interpersonal Privacy Profiles) that other users are in compliance with.

The Permission Satisfaction Score serves as a proxy for AR user experience, while the Privacy Satisfaction Score approximates how well bystanders' privacy expectations are met. Higher scores are favorable for both.

These scores play two key roles in our framework. First, they enable computing sensing policies that guarantee all users' individual UX or privacy requirements–expressed as per-user score thresholds–are upheld in Interaction-First and Privacy-First negotiations, respectively. For example, in the Privacy-First strategy, we can explore alternative combinations of sensing restrictions and evaluate their impact on each user's Permission and Privacy Satisfaction Scores; optimal solutions satisfy each user's Privacy Satisfaction threshold while minimizing reductions to the Permission Satisfaction Score (blue points along the Pareto Frontier in Fig. 5). We formulate these optimization problems in the next section.

Second, by strategically setting per-user thresholds, the scores enable expressing new kinds of optimization objectives implicitly. For example, in our earlier scenario, we could prioritize accessibility by assigning a high Permission Satisfaction threshold to the visually-impaired user relying on AR for safe navigation.

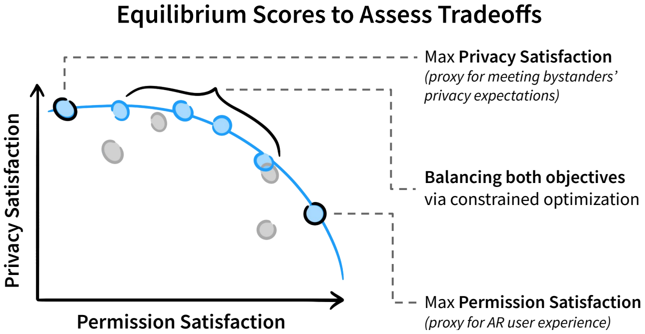


Figure 5: Equilibrium Scores to Assess Tradeoffs. We use the Permission and Privacy Satisfaction Scores to explore Equilibrium points along the Pareto Frontier. Each point represents a distinct negotiation strategy, where varying score thresholds lead to different UX–privacy tradeoffs. Blue circles highlight non-dominated points, which are optimal in the sense that no other point achieves better performance on the Interaction-First or Privacy-First objective without reducing performance on the other.

4.6 Optimization Algorithms

We have now established the core components of our framework: profiles to define users' requirements for AR Sensing and Interpersonal Privacy (Sec. 4.2), the Equilibrium Scope and Optimization Strategy dimensions (Sec. 4.3-4.4), and Equilibrium Scores (Sec. 4.5). Next, we describe the mathematical formulation and optimization algorithms that operationalize these concepts to determine a Privacy Equilibrium.

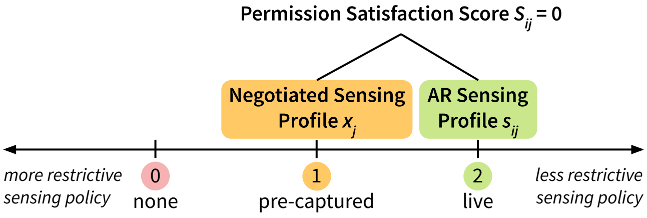

Permission Satisfaction Score $S_{ij} = 0$
Negotiated Sensing Profile x_j
AR Sensing Profile s_{ij}
more restrictive sensing policy
0
none
1
pre-captured
2
live
less restrictive sensing policy

Figure 6: AR Sensing Function Range. Sensing configurations towards the left are more restrictive, while the right tends to have higher Permission Satisfaction. If an AR Sensing Profile requests capturing live spatial mapping data, but the negotiated permission only grants access to pre-captured data, the Permission Satisfaction Score is 0.

4.6.1 Inputs. A user i's **AR Sensing Profile** for sensing function j can be written as $s_{ij} \in \{0, 1, \ldots, N\}$, where N is the number of possible configurations. Here, sensing function refers to a specific *data operation* (e.g., capturing, computing, or storing data) associated with an *AR sensing capability* (e.g., spatial mapping). As Figure 6 shows, if there are $N = 3$ settings for capturing spatial mapping data (not using this function, leveraging pre-captured data, or live data), s_{ij} could take on the corresponding values of $\{0, 1, 2\}$. Each sensing function j has an associated constant weight $0 \leq w_{ij} \leq 1$, with a higher value indicating that j is more critical to enabling user i's AR functionality. Our implementation uses a set of three weights to represent an intuitive priority of sensing capabilities: capabilities that are "Must Have", "Nice To Have", or that the AR app "Can Do Without" are weighted $\{0.6, 0.3, 0.1\}$ respectively. Appendix A.2 provides the AR Sensing Profile format as a C# class, along with an example profile for an Accessible Navigation app.

The **Interpersonal Privacy Profile** is defined similarly as $p_{ij} \in \{0, 1, \ldots, N\}$. For example, an AR user may request live spatial capture ($s_{ij} = 2$) as a crucial enabler of navigation functionality ($w_{ij} = 0.6$), while a co-located bystander prefers they use a previously saved environmental map ($p_{ij} = 1$). Each user also specifies a minimum Permission Satisfaction threshold $\mathcal{S}_i$ and a Privacy Satisfaction threshold $\mathcal{P}_i$ that they would like to achieve. Appendix A.3 provides an example Interpersonal Privacy Profile for a *Privacy Fundamentalist* persona [15]. Note that we assume each user runs one AR application, so we use the terms "user" and "application" interchangeably throughout this section. Our framework is extensible to users running multiple AR applications.

4.6.2 Outputs. Given a set of user profiles as input (where the user group is determined by the specified Equilibrium Scope), our optimization algorithm outputs the negotiated configuration x_j for each sensing function j. The final sensing configuration applied to each user i is $\min(s_{ij}, x_j)$ to ensure that an AR application is not granted more access than the user consents to, even if the negotiated configuration allows it (e.g., x_j permits live eye tracking, but the Navigation app does not require it).

4.6.3 Equilibrium Scores. Our framework is flexible and can incorporate different definitions of Equilibrium Scores (Sec. 4.5). Our current instantiation defines the **Permission Satisfaction Score** S_{ij} as whether the AR app's requirement for sensing function j is satisfied or not:

$$\text{Permission Satisfaction Score } S_{ij} = \begin{cases} 1 & \min(s_{ij}, x_j) \geq s_{ij} \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

As in Figure 6, if the negotiated spatial mapping setting is "pre-captured" ($x_j = 1$), but the Navigation app desired it to be live ($s_{ij} = 2$), then according to the second case in Equation 1, $S_{ij} = 0$.

Similarly, the **Privacy Satisfaction Score** P_{ij} can be defined as whether the user's desired privacy preferences are satisfied or not:

$$\text{Privacy Satisfaction Score } P_{ij} = \begin{cases} 1 & x_j \leq p_{ij} \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

For example, if a bystander prefers AR users to rely on pre-recorded spatial maps ($p_{ij} = 1$) to avoid being captured on live maps, and the negotiated sensing function is also pre-recorded ($x_j = 1$), then according to the first case in Equation 2, $P_{ij} = 1$.

4.6.4 Equilibrium Optimization Strategies. With this mathematical notation in hand, we can now describe the optimization strategies from Sec. 4.4 more precisely.

The **Ownership-Based** approach can be written as:

$$x_j = p_{i^* j} \tag{3}$$

where i^* is the space owner in the Space-Wide scope or a specific user who owns their proxemic zone in the Zone-Wide and Peer-to-Peer scopes. In other words, the negotiated sensing function is set to that of the owner's Interpersonal Privacy Profile.

The **Privacy-First** optimization problem can be written as:

$$\max_{x_j} \min_{i} \quad \sum_{j} w_{ij} S_{ij} \tag{4}$$

$$\text{subject to} \quad \sum_{j} P_{ij} \geq \mathcal{P}_i, \quad \forall i \tag{5}$$

$$(1), (2)$$

$$x_j, s_{ij}, p_{ij} \in \{0, 1, \ldots, N\}$$

The objective in Equation 4 is to maximize the lowest Permission Satisfaction Score across all users. This score is computed as the weighted sum of sensing function scores (S_{ij}; Eqn. 1), where each weight w_{ij} reflects how critical sensing function j is to user i's AR app. Intuitively, sensing functions most essential to app capabilities contribute more to the total Permission Satisfaction Score. We choose this form of the objective function for fairness, so that no user is "left behind," ending up with a much worse Permission Satisfaction Score than other users. The constraint in Equation 5 guarantees every user's Privacy Satisfaction Score meets their Privacy Satisfaction threshold, meaning their individual privacy requirements are not violated.

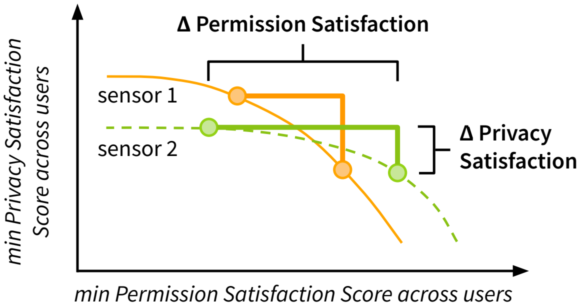


Figure 7: Cost function for Privacy-First optimization. Starting from a high privacy score on the left, we choose to loosen the sensing capability with the shallowest slope $\left(\max \frac{\Delta\text{Permission Satisfaction}}{1+\Delta\text{Privacy Satisfaction}}\right)$. In this example, the algorithm chooses sensor 2 (dashed green line) to loosen, as it incurs the smaller tradeoff between Permission Satisfaction and Privacy Satisfaction.

Algorithm for Privacy-First optimization. We model the Privacy-First strategy as an integer program, a class of NP-complete problems that are generally inefficient to solve exactly at scale. In our case, the AR Sensing Profile (Appendix A.2) defines $N = 21$ sensing functions: 7 sensing capabilities × 3 data operations (capture, computation, and storage of data). Each function has $M = 3$ options (e.g., live, pre-captured, or no data for the capture attribute). Brute-force enumeration would require exponential time, with $M^N \approx 10$ billion possibilities in the worst case.

Instead, we propose a greedy heuristic algorithm that considers configurations of allowed sensing capabilities along the Pareto Frontier via an epsilon-constrained approach, maximizing the Interaction-First objective while treating Privacy-First as a constraint (Eqn. 4-5). This algorithm is illustrated in Figure 7 and described in pseudocode in Appendix A.1. We start with an initial solution that maximizes all Privacy Satisfaction Scores by adopting the most restrictive set of sensing capabilities dictated by the involved users' Interpersonal Privacy Profiles. Then, we identify the most critical sensing capability to "loosen" by placing fewer restrictions on it (e.g., granting access to live spatial mapping instead of limiting AR apps to using pre-captured data). Here, we define the most critical capability as the one that yields the largest ratio of Permission Satisfaction Score to Privacy Satisfaction Score before and after loosening, evaluated for the user with the lowest score. In other words, we adjust sensing permissions to maximize gains in Permission Satisfaction while minimizing losses in Privacy Satisfaction. In the example shown in Figure 7, the algorithm selects sensor 2 (green line) to loosen, as it results in a greater increase in Permission Satisfaction (x-axis) and a smaller decrease in Privacy Satisfaction (y-axis) compared to sensor 1 (orange line). This search proceeds until all users meet their Permission Satisfaction thresholds or no sensing capabilities can be further loosened while satisfying all users' Privacy Satisfaction thresholds.

The **Interaction-First** problem is similar to Privacy-First, but instead treats the Permission Satisfaction Score as a constraint and the Privacy Satisfaction Score as the objective (Appendix A.1).

5 Privacy Equilibrium Toolkit

In this section, we present an instantiation of our Privacy Equilibrium framework in an interactive toolkit, consisting of a Unity simulation engine and a web-based visualization dashboard (Fig. 8). The toolkit enables simulating interactions between AR users and non-users across locations and experimenting with different strategies to reach a Privacy Equilibrium through a three-step process:

(1) **Establishing the scenario context by defining the physical environment, user movement patterns, and user profiles** (which reflect the AR application usage and privacy preferences of all individuals present in the environment);
(2) **Configuring the process for negotiating sensing capabilities to reach a Privacy Equilibrium**, in terms of users within the Equilibrium Scope (Sec. 4.3) and objectives to prioritize through Optimization Strategies (Sec. 4.4);
(3) **Assessing to what extent the desired Equilibrium point was reached**, by analyzing tradeoffs in UX and privacy for the current and prior optimization strategies.

We developed the toolkit with two goals in mind: (1) demonstrating the implementation feasibility and practical benefits of our conceptual framework; (2) providing a research platform for AR and S&P researchers and developers. Developers can use the toolkit to experiment with sensing requirements at the AR application level, assessing their impact on privacy with respect to various user needs and perceptions of privacy risks. As we approach the everyday use of AR, the toolkit also provides a basis for AR and S&P researchers to holistically explore and generate requirements for privacy mediation in the future AR ecosystem. Further information on the toolkit can be found at https://www.mi2lab.com/research/privacy-equilibrium.

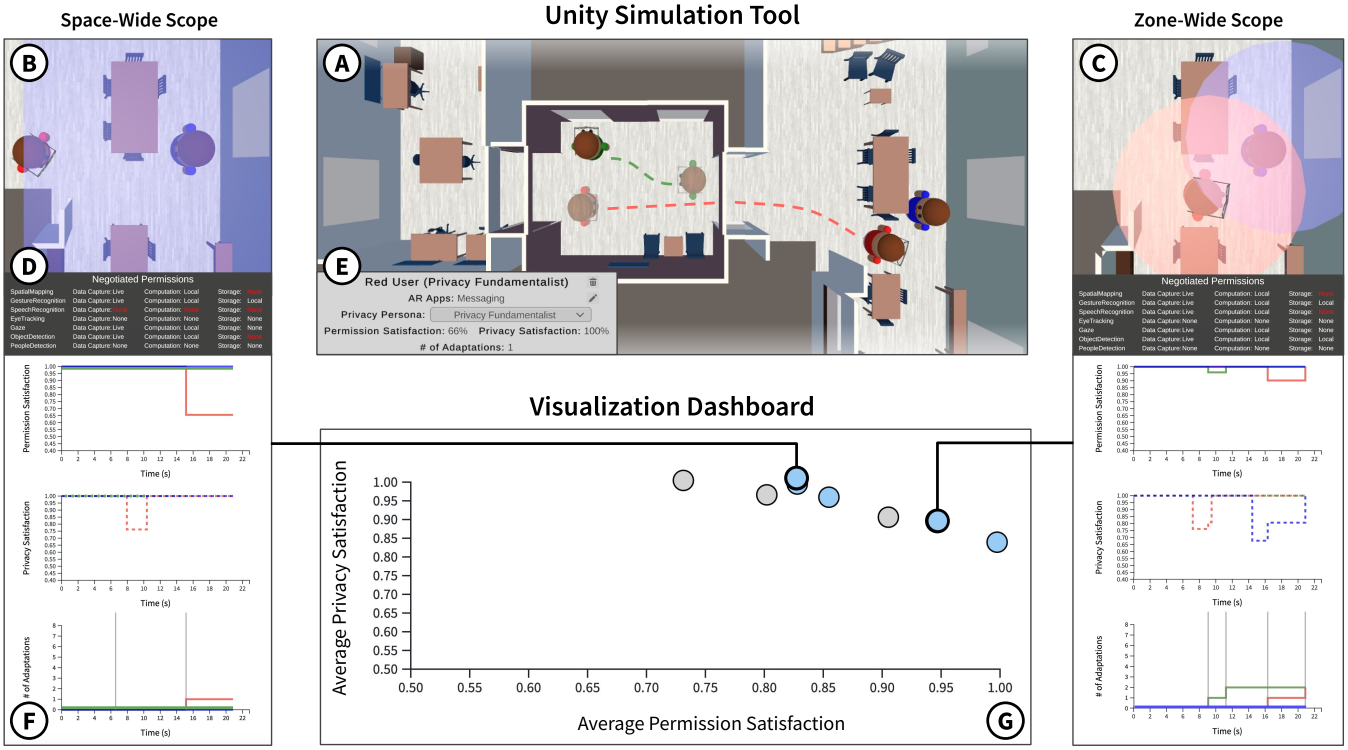
5.1 Step 1: Specifying the Context of Use

AR users' privacy expectations are shaped by their current tasks, both physical and virtual, and the social norms of the space they occupy [1, 16, 30]. Therefore, researchers or developers using our toolkit start by defining their scenario in terms of environments, user profiles, and interactions between users.

Our Unity simulation engine includes **mock physical environments represented as 3D floorplans**, including a hospital, classroom, and office (Fig. 8A). We generated these by scanning real-world spaces in Polycam[1] and exporting the captures to Unity. The environments prompt toolkit users to consider contextual factors when designing negotiation strategies according to our framework (e.g., the spatial layout and heightened privacy expectations within a hospital might suggest a Space-Wide, Privacy-First approach).

Our toolkit represents **AR users and non-users as avatars** with and without glasses in the scene, each characterized by an AR Sensing Profile and Interpersonal Privacy Profile. As described in Section 4.2, the AR Sensing Profile defines the required sensing capabilities for any AR applications in use (e.g., AR Telepresence, Accessible Navigation), while the Interpersonal Privacy Profile specifies capabilities a given user is comfortable with others around them using, based on a privacy persona [15] (e.g., the *Biometric Data-Concerned* user requests restrictions on speech recognition

[1] **Polycam:** https://poly.cam/



Negotiated Permissions

SpatialMapping	Data Capture: Live	Computation: Local	Storage: None
GestureRecognition	Data Capture: Live	Computation: Local	Storage: Local
SpeechRecognition	Data Capture: None	Computation: None	Storage: None
EyeTracking	Data Capture: None	Computation: None	Storage: None
Gaze	Data Capture: Live	Computation: Local	Storage: None
ObjectDetection	Data Capture: Live	Computation: Local	Storage: None
PeopleDetection	Data Capture: None	Computation: None	Storage: None

Red User (Privacy Fundamentalist)

AR Apps: Messaging

Privacy Persona: Privacy Fundamentalist

Permission Satisfaction: 66% Privacy Satisfaction: 100%

# of Adaptations: 1

Negotiated Permissions

SpatialMapping	Data Capture: Live	Computation: Local	Storage: None
GestureRecognition	Data Capture: Live	Computation: Local	Storage: Local
SpeechRecognition	Data Capture: Live	Computation: Local	Storage: None
EyeTracking	Data Capture: None	Computation: None	Storage: None
Gaze	Data Capture: Live	Computation: Local	Storage: None
ObjectDetection	Data Capture: Live	Computation: Local	Storage: Local
PeopleDetection	Data Capture: None	Computation: None	Storage: None

Figure 8: Privacy Equilibrium Toolkit Overview. Our toolkit includes a simulation engine implemented in Unity (A), which supports exploring AR usage behaviors and privacy risks across public environments, such as the office space shown here. Avatars representing users who leverage different AR applications and have varying privacy needs can be configured and animated to move around the space. Depending on the Equilibrium Scope, sensing negotiations are triggered when users enter designated regions (Space-Wide; B) or come into proximity with other people (Zone-Wide, Peer-to-Peer; C). The simulation engine supports real-time analysis of negotiated sensing capabilities (D) and Equilibrium Scores (E). A web-based dashboard enables post-hoc analysis of score trends over time (F) and comparison of UX-privacy tradeoffs incurred by different Optimization Strategies, visualized along a Pareto Curve (G).

and people detection). Users' profiles and positions in the scene can be configured via JSON files or created ad hoc during simulations.

Finally, we provide **animated motion sequences to simulate interactions between multiple users within the environment**. For example, Fig. 8A illustrates the red user leaving their office to get coffee, initiating a negotiation with the green user entering the elevator and later with the blue user in the kitchen.

Appendix A.4 demonstrates how to configure and define new user profiles and animation sequences in the simulation engine.

5.2 Step 2: Configuring the Negotiation Process

As animated user avatars move through the environment or enter each other's proximity, sensing negotiations are dynamically triggered based on the selected Equilibrium Scope and Optimization Strategy. Toolkit users can specify these dimensions, along with related parameters such as score thresholds, via dropdowns and input fields in the simulation engine UI (Fig. 11).

Equilibrium Scope: To compute when negotiations should occur and the users involved, we model spatial scopes using Unity's *collider* component. In the Space-Wide approach, large colliders are mapped to distinct areas of the environment (Fig. 8B), such as an office's lobby, kitchen, and lab space. For the Zone-Wide and Peer-to-Peer scopes, our toolkit anchors cylindrical colliders with a 4.5 meter radius to each user, approximating the spatial mapping range of commercially available AR glasses (Fig. 8C). For all three scopes, negotiations are triggered when people enter and exit the collision areas. To avoid repeated triggers from overlapping user-anchored zones, we implemented an algorithm to process related events concurrently.

Optimization Strategies: Given the user profiles of those within the Equilibrium Scope, our toolkit computes the negotiated set of sensing capabilities based on the specified strategy (Ownership-Based, Privacy-First, or Interaction-First). The outcome of these negotiations, compared against each user's ideal AR application permissions, is visualized through two UIs anchored to their avatar (Fig. 8D). One UI displays their AR Sensing Profile, and the other highlights any sensing restrictions in red. We implemented the Optimization Strategies in a C# utility according to the algorithms described in Section 4.6.

To refine the negotiation strategy and more closely approach their desired Equilibrium point, toolkit users can experiment with different thresholds for Permission and Privacy Satisfaction. The simulation engine UI supports setting these thresholds as values between 0 and 1, either globally (e.g., guaranteeing a Privacy Satisfaction Score of 0.9 for all users) or on a per-user basis (e.g., maximizing the Permission Satisfaction Score for users relying on AR for accessibility, while applying a lower threshold for less critical use cases like gaming).

5.3 Step 3: Analyzing UX & Privacy Tradeoffs

Finally, toolkit users can assess to what extent a Privacy Equilibrium has been reached through two sets of visualization features.

First, to support in-depth analysis of sensing capability negotiations, our Unity simulation engine provides **real-time views of Equilibrium Scores**. For each user, the toolkit computes the Permission and Privacy Satisfaction Scores, along with another metric called *Number of Adaptations*: the number of times each AR application must adjust its functionality to comply with the negotiated sensing policies throughout a usage session. This score provides another way to approximate impact on UX, in addition to Permission Satisfaction. We display these scores displayed on a per-user basis (Fig. 8E) along with averages, minimums, and maximums across all users (Fig. 11C).

Second, we developed a **web-based dashboard to support post-hoc analysis of tradeoffs** across different negotiation strategies through two types of visualizations:

(1) **Timeline Plots** show trends in user scores across multi-user interactions (Fig. 8F). For example, in the Space-Wide, Ownership-Based negotiation shown in Fig. 8B, the red AR User's Permission and Privacy Satisfaction are disproportionately impacted compared to other users, whereas the Zone-Wide approach leveraging Privacy-First optimization (Fig. 8C) requires all users to make some compromises.
(2) **Pareto Curves** visualize the UX-privacy tradeoffs of different Equilibrium points (Fig. 8G). Each point represents a unique negotiation strategy (varying Equilibrium Scope or score thresholds), plotted by the average Permission and Privacy Satisfaction Scores across all users. Points on the Pareto Frontier, where no other strategy outperforms them on both objectives, are highlighted in blue.

The Unity simulation records timestamped score data in log files, which toolkit users can upload and manually configure to create the dashboard visualizations.

6 Application Scenarios

To demonstrate the flexibility of our framework to resolve differences in multiple AR users' and bystanders' AR sensing requirements and privacy preferences, we walk through two application scenarios prototyped using our toolkit [23, 27]. Our goal in studying these scenarios was to understand the AR sensing capabilities negotiated by our optimization approach and assess how well they align with intuitive scenario needs.

We focus on two scenarios, set in a hospital and an office, that we designed to probe complex definitions for Privacy Equilibrium by highlighting different social norms and people with critical needs to use AR. In this section, we detail how we configured each scenario in Unity and systematically simulated negotiations with varying Equilibrium Scopes and Optimization Strategies. We compared UX-privacy tradeoffs using two analysis strategies enabled by our dashboard: one focused on timeline visualizations to capture high-level events and trends across users' scores (Sec. 6.1), and the other on Pareto Frontier plots that highlight tradeoffs between possible Equilibrium points (Sec. 6.2).

6.1 Hospital Scenario: Balancing Accessibility and Privacy

Aligned with our motivating scenario in the Introduction, we first explored how to prioritize accessibility and safety for a visually-impaired individual while mitigating privacy concerns inherently posed by assistive technologies.

Step 1: Specifying the Context of Use: Via the simulation engine, we designed a hospital environment with interactions between two people: *(1)* A low-vision person using an AR Navigation app (leveraging spatial mapping, people, and object detection) to find a table in the waiting area (Fig. 9; blue avatar); *(2)* Another visitor who is not using AR and is concerned about location-related data collection–they want to avoid being linked to a specific place or time (Fig. 9; pink avatar). We animated the Navigation user to slowly walk past the *Location-Concerned* bystander and change paths once their AR device detects a person.

Step 2: Configuring the Negotiation Process: To systematically explore negotiation strategies enabled by our framework and their ability to resolve conflicting user needs, we simulated different combinations of Equilibrium Scopes and Optimization Strategies. For the Privacy-First and Interaction-First optimization objectives, we used 4 threshold pairs for Permission and Privacy Satisfaction which proved to consistently produce distinct Equilibrium points across different user profiles (see Appendix A.5 for our threshold selection method). These thresholds were applied to all users. To maintain the low-vision user's Navigation functionality, we also included one example of per-user thresholds, guaranteeing them a Permission Satisfaction Score of at least 0.8 and a Privacy Satisfaction Score of at least 0.7 for the bystander. For the Ownership-Based strategy, we designed a policy that applies sensing restrictions aligned with users' privacy preferences (e.g., prohibiting location-related data collection in the waiting area).

Since our scenarios involved negotiations between just two users at a time, we only used the Space-Wide and Zone-Wide scopes; Peer-to-Peer typically produces the same output as Zone-Wide in such cases (Sec. 4.3). With 2 Scopes x 11 Optimization Strategies (5 threshold pairs each for Interaction-First and Privacy-First, plus 1 Ownership-Based policy), this resulted in 22 simulation trials.

Step 3: Analyzing UX and Privacy Tradeoffs: To identify which strategies balanced the needs of the visually-impaired user with the privacy concerns of the bystander, we used the dashboard to inspect timeline plots from the simulations that maintained a Permission Satisfaction Score of at least 0.8 for the low vision user. Since this score provides only a coarse-grained estimate of the impact on UX, we examined whether the specific permission restrictions in Unity aligned with our intuition of what sensing capabilities are required to maintain Navigation functionality (i.e., spatial mapping). Two trials met our selection criteria (Fig. 9), for which we make the following observations:

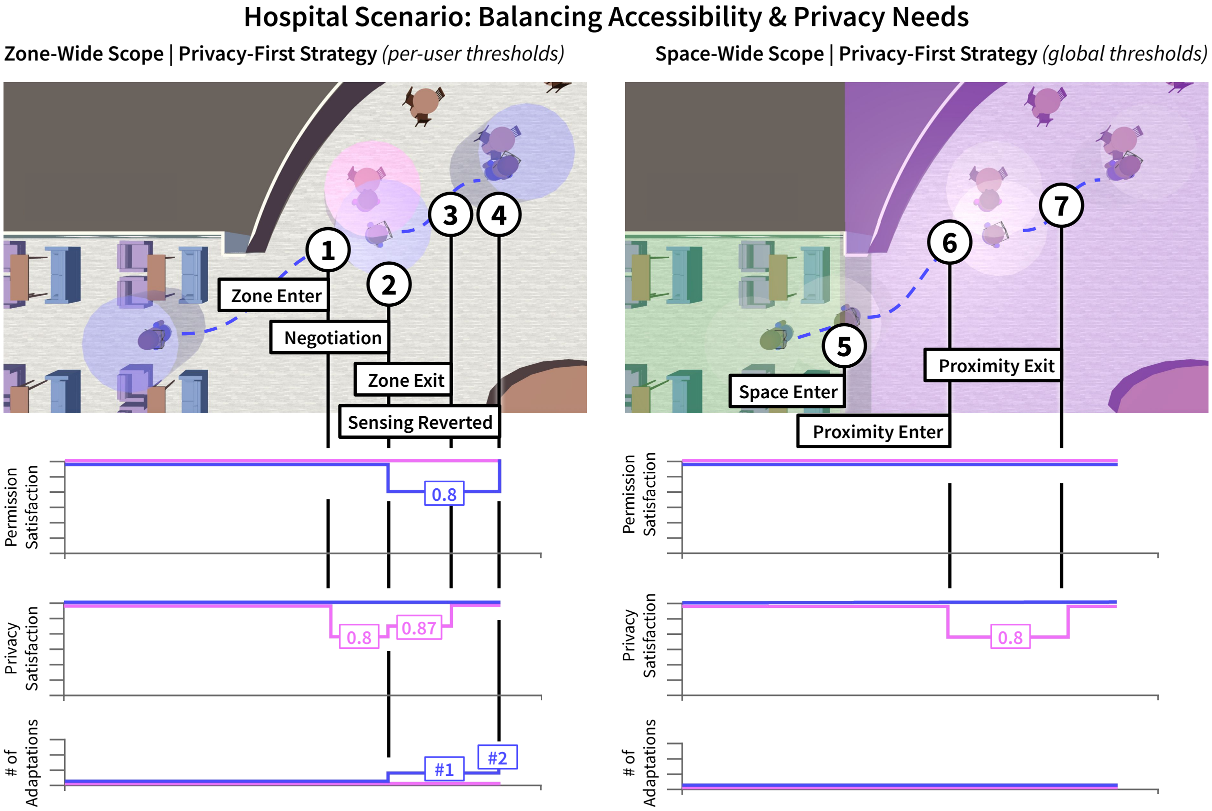


Figure 9: Application # 1: Visual Access in a Hospital Setting. Our experiments surfaced two negotiation strategies that enable a low-vision user (in blue) to safely navigate using AR while respecting the privacy preferences of a *Location-Concerned* bystander (in pink). In the Zone-Wide, Privacy-First approach on the left, a negotiation is triggered when the low-vision user comes near the bystander (1, 2), leading to a temporary restriction on people detection (while preserving safety-critical AR sensing capabilities like spatial mapping and object detection) until the people separate (3, 4). In the Space-Wide, Privacy-First approach on the right, users' Privacy Satisfaction thresholds are checked when the low vision user enters the waiting area (5); since no users would fall below their 0.8 threshold, no adjustments to the AR sensing capabilities are needed (6, 7).

(1) **The Zone-Wide, Privacy-First strategy with Per User Thresholds met the bystander's privacy concerns by downgrading the low-vision user's less essential sensing capabilities**. This strategy resulted in a 0.8 Permission Satisfaction Score for the low-vision user and 0.87 Privacy Satisfaction Score for the bystander (Fig. 9.2). The primary sensing restriction was on people detection; we considered this an acceptable tradeoff, as the Navigation app could still rely on spatial mapping and object detection to safely redirect the low-vision user during the short period of proximity to the bystander. The Zone-Wide scope avoided prematurely restricting AR functionality before a privacy concern arose, only adjusting AR sensing capabilities as the two users neared each other.

(2) **The Space-Wide, Privacy-First strategy proactively considered whether to adjust sensing capabilities to minimize bystander privacy risks.** We set a global threshold of 0.8 for both the Permission and Privacy Satisfaction Scores. As shown in Figure 9.5, the negotiation was triggered when the low-vision user entered the waiting area. AR functionality remained fully intact for the low-vision user, causing the bystander to experience a drop in Privacy Satisfaction to 0.8 (Fig. 9.6-7). However, we consider the bystander to be at low privacy risk due to the limited exposure period and the fact that their privacy requirements were not violated, as defined by their threshold.

Appendix A.5 provides a full walkthrough of how the Privacy-First algorithm (Alg. 1) determines negotiated sensing configurations for this scenario.

6.2 Office Scenario: Balancing Privacy Preferences at the Extremes

To assess the robustness of our optimization approach in bridging gaps between heterogeneous users, we explored a scenario with conflicting privacy preferences (ranging from unconcerned to highly concerned users).

Step 1: Specifying the Context of Use: This scenario was set in an office space (environment shown in Fig. 8). To isolate the effects of different privacy profile pairings, we simulated interactions between two people using the same AR Telepresence

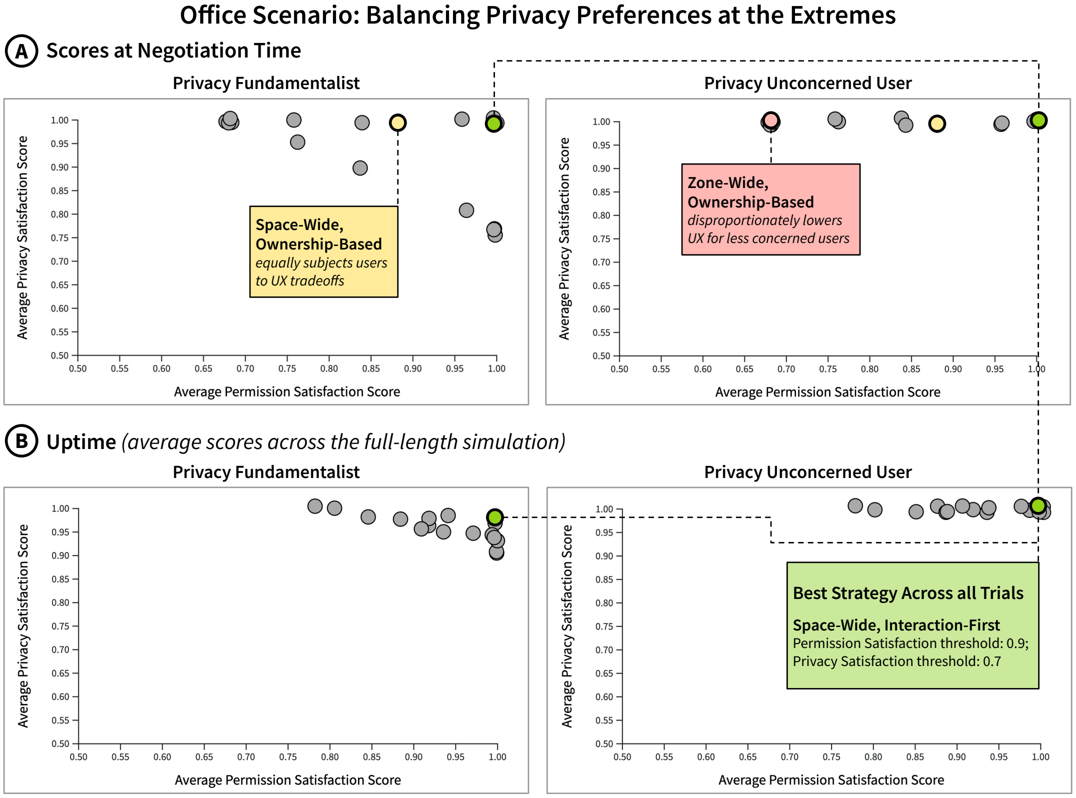


Figure 10: Application #2: Resolving Conflicting Privacy Preferences. Which strategies incur equal tradeoffs for UX and privacy when users have varying levels of concern? We simulated interactions between two privacy personas pairs: {*Fundamentalist* x *Biometric-Concerned*} and {*Fundamentalist* x *Unconcerned*}. For the latter pair, we plot the per-user Permission and Privacy Satisfaction Scores immediately after a negotiation (A) and as averages across the multi-user interaction (B). Our analysis shows that Space-Wide scope effectively balanced users' conflicting preferences, while Ownership-Based approaches led to lower Permission Satisfaction Scores, disproportionately affecting the *Unconcerned* user in the Zone-Wide approach.

app, animating one user to enter the lab space and sit down at a desk, while crossing paths with an existing user in the office. The pairings included a highly risk-averse *Privacy Fundamentalist* and a *Privacy Unconcerned* user, as well as the *Fundamentalist* paired with a *Biometric-Concerned* user who is averse to sensing that could reveal their identity or personal characteristics.

Step 2: Configuring the Negotiation Process: Using the same procedure as our first application scenario, we simulated multi-user interactions with different Equilibrium Scopes crossed with Optimization Strategies, using varying Permission and Privacy Satisfaction thresholds. For the Space-Wide Ownership-Based approach, we applied a zone over the office that restricts biometric data collection. Across all the different pairings, this resulted in 34 simulation trials.

Step 3: Analyzing UX and Privacy Tradeoffs: To analyze whether each strategy impacted users in a balanced or imbalanced manner, we plotted the individual Permission and Privacy Satisfaction Scores in two ways: immediately after the negotiation, and averaged over the full simulation duration (which we call "uptime"). We made three main observations, illustrated in Fig. 10 for the privacy personas at the extremes (*Fundamentalist* and *Unconcerned*).

- **The Space-Wide, Interaction-First strategy minimized degradations to UX and privacy.** It produced the only non-dominated point on the Pareto Frontier across all simulation configurations (green point in the upper right corner of each plot), suggesting it resolved differences in users' conflicting privacy needs in a balanced manner. However, we note that over multi-user interactions of a longer duration, the Permission Satisfaction uptime may decline (shifting left in Fig. 10B). This is because the Space-Wide scope restricts AR sensing capabilities even when users' devices are not within proximity of each other.
- **The Space-Wide, Ownership-Based strategy—representative of World-Driven Access Control [39]—subjected all users to equal UX tradeoffs.** Note that under this strategy (yellow points in Fig. 10A), the tradeoffs will vary based on the set of allowed AR sensing capabilities in a given space. We simulated a moderate policy in line with the *Biometric-Concerned* profile; nevertheless, our Interaction-First optimization approach achieved a better tradeoff for users with more extreme privacy preferences.
- **The Zone-Wide, Ownership-Based approach disproportionately impacted UX for less privacy-concerned users.** This is

evident in the *Fundamentalist's* Permission Satisfaction Score remaining at 1.0, while the *Unconcerned* user's score dropped to 0.68 when using the same AR application (red point in Fig. 10A). While the combination of Zone-Wide scope with Ownership-Based optimization is ideal for granting users control over their privacy in personal spaces (e.g., a private office), our results suggest it may be less viable in shared public environments.

7 Walkthrough of Privacy Equilibrium Toolkit with Security & Privacy Experts

To further validate our framework and elicit improvements for its instantiation within our toolkit, we conducted a walkthrough evaluation [27] with eight researchers specializing in S&P and AR-related technologies. We chose to work with researchers as they represent a primary class of target users for our toolkit, which we intend as a platform for prototyping privacy-mediating techniques for everyday AR and exploring the sociotechnical implications in different scenarios. In line with this goal, our study tasked the researchers with using our toolkit to compare sensing negotiation strategies for our hospital and office scenarios and assessing to what extent they balanced competing user needs.

7.1 Participants

Through our professional networks, we recruited eight researchers with core expertise in security and privacy, along with experience working on AR or related technologies such as IoT and cloud systems. This included four professors and four late-stage PhD students (mean age of 36; two preferred not to report). Three participants had 3+ years of S&P research experience; five had 5+ years across venues such as CHI, USENIX Security, SOUPS, and ISMAR.

7.2 Method

We conducted individual, 1-hour study sessions over Zoom. Participants were compensated with $20 USD gift vouchers for their time. We centered our studies around the two scenarios used in our application demonstration (Sec. 6), involving AR users and non-users who have conflicting UX and privacy goals in two environments:

(1) **Hospital Waiting Area**: A visually-impaired person using AR for navigation passes by a *Location-Concerned* bystander who wants to prevent others from inferring their activities in the space (Fig. 9).
(2) **Office Space**: Two AR users with contrasting privacy preferences–a risk-averse *Privacy Fundamentalist* and a *Privacy Unconcerned* user–cross paths with each other, as well as a *Biometric Data-Concerned* bystander who is averse to sensing that could reveal their identity or personal characteristics (Fig. 8).

Using our toolkit to demonstrate each scenario, we guided participants through two tasks: *(1)* defining what constitutes a balance between the involved users' UX and privacy needs and how sensing policies could be adjusted to achieve it; *(2)* reviewing three examples of negotiation strategies and assessing to what extent each achieves the desired Privacy Equilibrium defined in Task 1. The S&P experts completed both tasks for one scenario, then repeated both for the second scenario, with the scenario order counterbalanced between participants.

Task 1: Analyzing Scenario-Dependent Conditions for Equilibrium *(5 min per scenario):* The goal of the first task was to establish a baseline understanding, from the S&P experts' perspectives, of what achieving a Privacy Equilibrium would require in each scenario. We used the Unity simulation engine to present each user's AR sensing requirements and privacy preferences, and played animation sequences showing how users moved through the space. Then, we asked the experts to assess to what extent a balance already exists between the UX and privacy needs of all people in the space. If they perceived an imbalance, they identified specific points in the animation where adjusting the use of AR sensing capabilities could help achieve a balance. To avoid biasing their assessments, we hid simulation features that explicitly referenced components of our framework, such as zones and score visualizations.

Task 2: Reviewing and Ranking Strategies to Establish a Privacy Equilibrium *(20 min per scenario):* To understand how the S&P experts would leverage different features of the toolkit to weigh the benefits and limitations of various negotiation strategies, we presented them with three examples that represented non-dominated points on the Pareto Frontier (Fig. 5), but had very different implications for users' UX and privacy. To find these examples, we systematically ran optimizations with different thresholds for the hospital and office scenarios (described in Sec.6.1) and filtered out trials that produced identical Permission and Privacy Satisfaction averages. Then, we then selected two Equilibrium points from the extremes of the tradeoff curve (maximizing Permission and Privacy Satisfaction) and one from the middle (balancing the two).

We demonstrated the strategies one at a time via the Unity simulation engine, bringing back visualizations of the zones, AR Sensing Profiles, and Equilibrium scores. This helped the S&P experts understand the AR glasses' sensing range, when users entered and exited proximity, and the impact of specific negotiated sensing policies. Before moving to the next strategy, experts inspected the timeline plots of Equilibrium scores in our dashboard, thinking aloud to describe any patterns they could see. After the second and third strategies, we asked them to discuss whether the new strategy achieved a better UX-privacy tradeoff than the previous, based on their usage and understanding of the toolkit features.

Discussion *(10 min):* We ended with a discussion to understand the benefits and limitations of key components of our framework: *(1)* Inputs to our optimization strategies, including user profiles for sensing capabilities and privacy preferences, users' movement data, and customizable thresholds for Permission and Privacy Satisfaction; *(2)* Equilibrium scores to assess UX-privacy tradeoffs (Sec. 4.5). Lastly, the experts reflected on pros and cons of the toolkit features for interpreting the scenario context and evaluating the effectiveness of the optimization strategies.

7.3 Data Collection & Analysis

We captured screen and audio recordings of study sessions for later analysis. During each session, the experimenter noted observations on the experts' toolkit usage behaviors, based on which features they were interacting with or referring to during via think-aloud. We used an affinity diagramming approach [44] to extract and consolidate themes from audio transcripts and notes.

7.4 Results

We organize our findings into four themes that capture how the S&P experts assessed the Privacy Equilibrium framework and engaged with the toolkit. First, we discuss the expressiveness of our optimization approach for balancing competing user needs, and the effectiveness of our metrics in modeling UX and privacy tradeoffs.

Theme 1: Benefits of our framework in enabling flexible and fine-grained sensing negotiation. Experts emphasized the need for granular control over how and to whom sensing restrictions are applied, and identified multiple components of our framework that support such control. In terms of the Equilibrium scope dimension, the Zone-Wide approach was perceived to offer the most flexibility (E1, E5, E7). In contrast with the Space-Wide scope, E1 noted that users in distant zones "can just live their lives... rather than having to restrict a sensor that can't even collect data [from] the area that's private." Experts also appreciated the user agency afforded by the Privacy-First and Interaction-First optimization strategies: "[all] users have some say in" the negotiation by customizing Permission and Privacy Satisfaction thresholds (E4).

Beyond explicitly calling for flexible AR access control, experts demonstrated this need by proposing many distinct Equilibrium definitions across the two scenarios, each of which could be expressed and evaluated within our framework. When potential consequences of privacy violations were unclear, many chose to "err on the side of [caution]" (E7), favoring strategies that fully maximized Privacy Satisfaction (E5–8). In such cases where UX tradeoffs were necessary, experts had two contrasting proposals: distributing costs evenly across all AR users (E1, E3, E4) or or concentrating costs on a few users to minimize the number negatively impacted (E2, E8). The exception was the low-vision user in the hospital scenario, for whom experts prioritized maintaining full functionality.

Theme 2: Limitations of our framework in modeling the impact of sensing restrictions and severity of private data exposure. All experts were able to use the Permission and Privacy Satisfaction Scores to gauge which strategies aligned with their definitions for Privacy Equilibrium from Task 1. However, they noted these scores only provide a coarse-grained approximation of the impact of sensing negotiations, wanting finer-grained insight into potential adverse effects on both UX and privacy. As E4 put it, this requires modeling the "the semantics" of how AR applications leverage sensing capabilities, "not just the syntax."

In terms of UX, experts wanted to understand how AR applications adapt to sensing restrictions (E1-4), and if a user "loses access to information" or key functionality, "how vulnerable" they become (E1), particularly for the low-vision user in the hospital scenario.

On the privacy side, experts sought more details on the granularity of data captured by AR apps and the likelihood of leaking bystander data (E1-2, E5-6, E8), based on data storage and retention policies (E2-4). They also stressed that "a number on [privacy] is just not enough" (E7) to capture nuances in users' perception of experiencing a privacy violation (E2-3, E7). As E2 expressed, "what does 15% uncomfortable vs. 30% mean?" E7 also noted the asymmetric nature of the Privacy vs. Permission Satisfaction Scores: with privacy, "once you lose something, it's lost. UX can be recovered."

Finally, we present two themes around the types of analysis our toolkit enabled and discuss opportunities for improvement.

Theme 3: Simulated motion paths, zones, and in-situ score visualizations supported analyzing scenarios with multiple levels of abstraction. The Unity simulation engine effectively conveyed the context of each scenario, allowing S&P experts to understand sensing negotiations and reason beyond what was explicitly shown. Visualizing motion paths and zone intersections not only helped them identify when and where negotiations occurred, but also assess potential exposure of private data based on AR devices' sensing range and user orientation (E1–2, E4, E6–8). For example, E4 and E8 considered the hospital bystander to have low privacy risk since they were not facing the AR user. The AR Sensing Profile UIs anchored to users also supported different types of analysis: some experts gauged sensing restrictions at a high level by tracking color changes from red to white (E1, E3, E7), while others zoomed in to weigh the impact of specific restricted capabilities.

To more accurately model how AR interfaces adapt and the severity of data exposure, experts suggested visualizing AR users' first-person perspective (E2) and sensors' fields of view (E6).

Theme 4: Timeline visualizations of scores enabled "local planning vs. global planning" (E5). Similarly, the dashboard's timeline plots enabled analyzing UX-privacy tradeoffs at multiple time scales. All experts examined the height of "dents" (E3) in the Permission and Privacy Satisfaction timelines to assess the impact of negotiations on individual users. Many also considered the duration of score drops (E2–E5, E7–E8) to evaluate which strategies were more "efficient in regaining the original values" (E3). Beyond individual negotiations, the timelines enabled broader assessments of balance and fairness by making visible how many users were affected and how often their scores dipped throughout the scenario.

To better enable toolkit users to simultaneously perform local and global analysis, E1 proposed embedding videos of negotiations from the simulation engine within the dashboard.

7.5 Study Limitations

We note two main limitations of our studies: the generalizability of our results to real-world AR usage scenarios and to toolkit users without S&P expertise.

Generalizability of scenarios: The scenarios explored in our application walkthroughs (Sec.6) and studies with S&P researchers were limited in number and scope, focusing primarily on public contexts and involving a small set of simulated AR users and non-users. While we took steps to represent users realistically (e.g., recording motion paths through real physical environments, developing privacy personas based on empirical surveys of end-users' perceptions of risk [15, 16, 30]), our insights into the benefits and limitations of different negotiation strategies may not generalize as AR devices become more widely available and privacy attitudes evolve. We see potential in our toolkit to help bridge these gaps in understanding as the AR landscape advances, as it was designed to be extensible for modeling novel scenarios (through specifying new usage contexts, AR device capabilities, and privacy personas).

Study sample: The study involved researchers whose primary expertise lies in security & privacy, applied to AR, IoT, and related technologies. Some participants reported having high standards for protecting their own privacy, which at times led them to prefer optimization strategies that prioritized minimizing privacy risks over preserving UX. As such, their perspectives may not fully reflect those of other toolkit users, such as AR system designers who may be inclined to prioritize usability or implementation feasibility.

8 Discussion

Throughout our development of the Privacy Equilibrium framework and studies with S&P experts, we used simulation [28] to evaluate the flexibility of our optimization approach and probe into sociotechnical considerations for privacy mediation in AR (e.g., how different environments shape privacy norms, and what constitutes a “fair” balance for users with conflicting needs). While such explorations are not yet feasible in realistic usage settings, due to a limited AR user base and the lack of cross-platform infrastructure to communicate negotiation inputs and outputs, they raised important questions on what it would take to translate our framework's underlying concepts to future AR use: How can we elicit privacy preferences from AR users and bystanders in dynamic contexts, model associated risks with higher granularity, and convey to AR users how negotiations affect their AR experiences?

We reflect on these questions relative to our current implementation of the framework and suggest research directions to bridge the gap to real-world implementation.

Enabling AR users & bystanders to participate and express preferences for negotiations. As inputs to negotiations, we rely on user profiles that define their AR sensing requirements (specified by AR application developers) and privacy preferences towards others who may be sensing in the same environment (specified by AR users). To align with prior access control frameworks (Sec. 2.2) and to support compatibility with today's AR applications, we format these profiles as permission models–sets of sensing capabilities that can be granted to or restricted from AR applications. However, a limitation is that these models are not easily human-understandable, and would likely require users to have technical knowledge of AR and associated privacy risks.

Our toolkit demonstrates one way to lessen users' burden: allowing them to select Interpersonal Privacy Profiles aligned with privacy personas [15] that reflect their typical behaviors. However, this barrier must be further lowered as AR is increasingly used in everyday settings, as users will have limited “compliance budgets” (time and effort) to manage their context-dependent privacy needs, especially in dynamic environments [5]. We see potential to apply recent approaches that model privacy preferences based on past perceptions of risk [48], but note that such personalization techniques can also introduce new privacy risks. Future work should explore interaction techniques and technical requirements for AR non-users to participate in negotiations (e.g., broadcasting privacy preferences and proximity data via Bluetooth on their phones).

Fine-grained modeling of AR user experience and privacy risks. To enable modeling AR sensing negotiations as constrained optimization problems, we designed our Equilibrium Scores to be easily computed from user profiles and expressed as clear thresholds representing UX and privacy expectations. However, as noted by the S&P experts, these single-value metrics do not fully capture the nuance of how AR interfaces are affected by sensing restrictions, or when interactions with other AR users might pose privacy risks. Experts suggested modeling UX satisfaction at the level of adaptation techniques [34] (e.g., measuring users' reaction time or task performance when switching interaction modalities to cope with a sensing restriction). On the privacy side, they recommended modeling the severity of specific threats (e.g., speech recognition picking up a social security number versus a casual chat with friends). While we see the merit of this approach from a simulation perspective to better understand the pros and cons of negotiation strategies, we anticipate potential S&P risks for real-world implementation. For example, requiring AR apps to disclose which privacy-enhancing technologies or adaptation techniques they support could make new attack vectors visible. Similarly, if a centralized negotiation engine must detect and interpret data types that users deem sensitive, it may risk exposing even more personal information.

Conveying the impact of negotiations to AR users. Finally, we see a need for future work on explainability techniques [47] to help AR users understand why and how their functionality is adapted to preserve privacy. Our simulations suggest that with Zone-Based scopes or crowded environments, functionality may be frequently granted, degraded, or reverted based on ongoing negotiations. As such, it is critical to explore techniques that minimize disruptions to UX (e.g., guiding users through AR interface transitions) and enhance transparency (e.g., informing users of the benefits they gain from privacy-preserving measures).

9 Conclusion

This paper introduced the Privacy Equilibrium framework for balancing privacy in multi-user AR scenarios, using constrained optimization to facilitate system-driven negotiations of AR sensing capabilities. Our framework formalizes definitions for Equilibrium Scopes, Optimization Strategies, Equilibrium Scores to assess tradeoffs between UX and privacy. Based on this framework, we developed a simulation and analysis toolkit to prototype and evaluate different negotiation strategies across multi-user scenarios. Our application demonstrations, set in hospital and office environments, illustrated our framework's flexibility to resolve conflicting user needs, and walkthroughs with S&P researchers surfaced initial feedback to improve our toolkit. Future work could investigate deeper modeling of interface-level AR adaptations and data exposure, as well as mixed-initiative approaches to increase end-users' awareness and control over the negotiation process.

References

[1] Melvin Abraham, Mohamed Khamis, and Mark McGill. 2024. Don't Record My Private pARts: Understanding The Role of Sensitive Contexts and Privacy Perceptions in Influencing Attitudes Towards Everyday Augmented Reality Sensor Usage. In *IEEE International Symposium on Mixed and Augmented Reality, ISMAR 2024, Bellevue, WA, USA, October 21-25, 2024*. IEEE, 749–758. https://doi.org/10.1109/ISMAR62088.2024.00090

[2] Melvin Abraham, Mark McGill, and Mohamed Khamis. 2024. What You Experience is What We Collect: User Experience Based Fine-Grained Permissions for Everyday Augmented Reality. In *Proceedings of the CHI Conference on Human Factors in Computing Systems, CHI 2024, Honolulu, HI, USA, May 11-16, 2024*. ACM, 772:1–772:24. https://doi.org/10.1145/3613904.3642668

[3] Melvin Abraham, Pejman Saeghe, Mark McGill, and Mohamed Khamis. 2022. Implications of XR on Privacy, Security and Behaviour: Insights from Experts. In

NordiCHI '22: Nordic Human-Computer Interaction Conference, Aarhus, Denmark, October 8 - 12, 2022. ACM, 30:1–30:12. https://doi.org/10.1145/3546155.3546691

[4] Devon Adams, Alseny Bah, Catherine Barwulor, Nureli Musaby, Kadeem Pitkin, and Elissa M. Redmiles. 2018. Ethics Emerging: the Story of Privacy and Security Perceptions in Virtual Reality. In *Fourteenth Symposium on Usable Privacy and Security, SOUPS 2018, Baltimore, MD, USA, August 12-14, 2018.* USENIX Association, Berkeley, CA, USA, 427–442. https://www.usenix.org/conference/soups2018/presentation/adams

[5] Adam Beautement, Martina Angela Sasse, and Mike Wonham. 2008. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 Workshop on New Security Paradigms, Lake Tahoe, CA, USA, September 22-25, 2008.* ACM, 47–58. https://doi.org/10.1145/1595676.1595684

[6] Divyanshu Bhardwaj, Alexander Ponticello, Shreya Tomar, Adrian Dabrowski, and Katharina Krombholz. 2024. In Focus, Out of Privacy: The Wearer's Perspective on the Privacy Dilemma of Camera Glasses. In *Proceedings of the CHI Conference on Human Factors in Computing Systems, CHI 2024, Honolulu, HI, USA, May 11-16, 2024.* ACM, 577:1–577:18. https://doi.org/10.1145/3613904.3642242

[7] Ann Cavoukian. 2010. Privacy by Design: The 7 Foundational Principles. Revised: October 2010.

[8] Ruei-Che Chang, Yuxuan Liu, and Anhong Guo. 2024. WorldScribe: Towards Context-Aware Live Visual Descriptions. In *Proceedings of the 37th Annual ACM Symposium on User Interface Software and Technology, UIST 2024, Pittsburgh, PA, USA, October 13-16, 2024.* ACM, 140:1–140:18. https://doi.org/10.1145/3654777.3676375

[9] Kaiming Cheng, Mengyu Chen, Feiyu Lu, Youngwook Do, and Blair MacIntyre. 2024. SpatialPrivacy: Spatial Sharing for Remote Collaboration in Mixed Reality. In *2024 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct).* 9–11. https://doi.org/10.1109/ISMAR-Adjunct64951.2024.00009

[10] Ji-Won Chung, Xiyu Jenny Fu, Zachary Deocadiz-Smith, Malte F. Jung, and Jeff Huang. 2023. Negotiating Dyadic Interactions through the Lens of Augmented Reality Glasses. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference, DIS 2023, Pittsburgh, PA, USA, July 10-14, 2023.* ACM, 493–508. https://doi.org/10.1145/3563657.3595967

[11] Matthew Corbett, Brendan David-John, Jiacheng Shang, Y. Charlie Hu, and Bo Ji. 2023. BystandAR: Protecting Bystander Visual Data in Augmented Reality Systems. In *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services* (Helsinki, Finland) *(MobiSys '23).* Association for Computing Machinery, New York, NY, USA, 370–382. https://doi.org/10.1145/3581791.3596830

[12] Jaybie A. de Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. 2020. Security and Privacy Approaches in Mixed Reality: A Literature Survey. *ACM Comput. Surv.* 52, 6 (2020), 110:1–110:37. https://doi.org/10.1145/3359626

[13] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In Situ with Bystanders of Augmented Reality Glasses: Perspectives on Recording and Privacy-Mediating Technologies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14).* Association for Computing Machinery, New York, NY, USA, 2377–2386. https://doi.org/10.1145/2556288.2557352

[14] Roy Dong, Lillian J. Ratliff, Alvaro A. Cárdenas, Henrik Ohlsson, and S. Shankar Sastry. 2018. Quantifying the Utility-Privacy Tradeoff in the Internet of Things. *ACM Trans. Cyber Phys. Syst.* 2, 2 (2018), 8:1–8:28. https://doi.org/10.1145/3185511

[15] Janna Lynn Dupree, Richard Devries, Daniel M Berry, and Edward Lank. 2016. Privacy personas: Clustering users via attitudes and behaviors toward security practices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems.* 5228–5239.

[16] Andrea Gallardo, Chris Choy, Jaideep Juneja, Efe Bozkir, Camille Cobb, Lujo Bauer, and Lorrie Cranor. 2023. Speculative Privacy Concerns about AR Glasses Data Collection. *Proc. Priv. Enhancing Technol.* 2023, 4 (2023), 416–435. https://doi.org/10.56553/popets-2023-0117

[17] Hilda Hadan, Derrick M. Wang, Lennart E. Nacke, and Leah Zhang-Kennedy. 2024. Privacy in Immersive Extended Reality: Exploring User Perceptions, Concerns, and Coping Strategies. In *Proceedings of the CHI Conference on Human Factors in Computing Systems, CHI 2024, Honolulu, HI, USA, May 11-16, 2024.* ACM, 784:1–784:24. https://doi.org/10.1145/3613904.3642104

[18] Aleksi Ikkala, Florian Fischer, Markus Klar, Miroslav Bachinski, Arthur Fleig, Andrew Howes, Perttu Hämäläinen, Jörg Müller, Roderick Murray-Smith, and Antti Oulasvirta. 2022. Breathing Life Into Biomechanical User Models. In *The 35th Annual ACM Symposium on User Interface Software and Technology, UIST 2022, Bend, OR, USA, 29 October 2022 - 2 November 2022.* ACM, 90:1–90:14. https://doi.org/10.1145/3526113.3545689

[19] Gaurav Jain, Basel Hindi, Zihao Zhang, Koushik Srinivasula, Mingyu Xie, Mahshid Ghasemi, Daniel Weiner, Sophie Ana Paris, Xin Yi Therese Xu, Michael C. Malcolm, Mehmet Kerem Türkcan, Javad Ghaderi, Zoran Kostic, Gil Zussman, and Brian A. Smith. 2024. StreetNav: Leveraging Street Cameras to Support Precise Outdoor Navigation for Blind Pedestrians. In *Proceedings of the 37th Annual ACM Symposium on User Interface Software and Technology, UIST 2024, Pittsburgh, PA, USA, October 13-16, 2024.* ACM, 139:1–139:21. https://doi.org/10.1145/3654777.3676333

[20] Suman Jana, David Molnar, Alexander Moshchuk, Alan Dunn, Benjamin Livshits, Helen J. Wang, and Eyal Ofek. 2013. Enabling Fine-Grained Permissions for Augmented Reality Applications with Recognizers. In *22nd USENIX Security Symposium (USENIX Security 13).* USENIX Association, Washington, D.C., 415–430. https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/jana

[21] Yunhan Jack Jia, Qi Alfred Chen, Shiqi Wang, Amir Rahmati, Earlence Fernandes, Zhuoqing Morley Mao, and Atul Prakash. 2017. ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms. In *24th Annual Network and Distributed System Security Symposium, NDSS 2017, San Diego, California, USA, February 26 - March 1, 2017.* The Internet Society. https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/contexlot-towards-providing-contextual-integrity-appified-iot-platforms/

[22] Christoph Albert Johns, João Marcelo Evangelista Belo, Anna Maria Feit, Clemens Nylandsted Klokmose, and Ken Pfeuffer. 2023. Towards Flexible and Robust User Interface Adaptations With Multiple Objectives. In *Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology, UIST 2023, San Francisco, CA, USA, 29 October 2023- 1 November 2023.* ACM, 108:1–108:17. https://doi.org/10.1145/3586183.3606799

[23] Dan R. Olsen Jr. 2007. Evaluating user interface systems research. In *Proceedings of the 20th Annual ACM Symposium on User Interface Software and Technology, Newport, Rhode Island, USA, October 7-10, 2007*, Chia Shen, Robert J. K. Jacob, and Ravin Balakrishnan (Eds.). ACM, 251–258. https://doi.org/10.1145/1294211.1294256

[24] Yoonsang Kim, Sanket Goutam, Amir Rahmati, and Arie E. Kaufman. 2023. Erebus: Access Control for Augmented Reality Systems. In *32nd USENIX Security Symposium, USENIX Security 2023, Anaheim, CA, USA, August 9-11, 2023*, Joseph A. Calandrino and Carmela Troncoso (Eds.). USENIX Association. https://www.usenix.org/conference/usenixsecurity23/presentation/kim-yoonsang

[25] Sarah Claudia Krings and Enes Yigitbas. 2024. TARPS: A Toolbox for Enhancing Privacy and Security for Collaborative AR. *Proc. ACM Hum.-Comput. Interact.* 8, EICS, Article 251 (June 2024), 22 pages. https://doi.org/10.1145/3660251

[26] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2018. Towards Security and Privacy for Multi-user Augmented Reality: Foundations with End Users. In *2018 IEEE Symposium on Security and Privacy, SP 2018, Proceedings, 21-23 May 2018, San Francisco, California, USA.* IEEE Computer Society, New York, NY, USA, 392–408. https://doi.org/10.1109/SP.2018.00051

[27] David Ledo, Steven Houben, Jo Vermeulen, Nicolai Marquardt, Lora Oehlberg, and Saul Greenberg. 2018. Evaluation Strategies for HCI Toolkit Research. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, CHI 2018, Montreal, QC, Canada, April 21-26, 2018*, Regan L. Mandryk, Mark Hancock, Mark Perry, and Anna L. Cox (Eds.). ACM, 36. https://doi.org/10.1145/3173574.3173610

[28] Roderick Murray-Smith, Antti Oulasvirta, Andrew Howes, Jörg Müller, Aleksi Ikkala, Miroslav Bachinski, Arthur Fleig, Florian Fischer, and Markus Klar. 2022. What simulation can do for HCI research. *Interactions* 29, 6 (2022), 48–53. https://doi.org/10.1145/3564038

[29] Vivek C. Nair, Gonzalo Munilla Garrido, and Dawn Song. 2023. Going Incognito in the Metaverse: Achieving Theoretically Optimal Privacy-Usability Tradeoffs in VR. In *Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology, UIST 2023, San Francisco, CA, USA, 29 October 2023- 1 November 2023.* ACM, 61:1–61:16. https://doi.org/10.1145/3586183.3606754

[30] Joseph O'Hagan, Pejman Saeghe, Jan Gugenheimer, Daniel Medeiros, Karola Marky, Mohamed Khamis, and Mark McGill. 2022. Privacy-Enhancing Technology and Everyday Augmented Reality: Understanding Bystanders' Varying Needs for Awareness and Consent. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 6, 4 (2022), 177:1–177:35. https://doi.org/10.1145/3569501

[31] Joon Sung Park, Joseph C. O'Brien, Carrie Jun Cai, Meredith Ringel Morris, Percy Liang, and Michael S. Bernstein. 2023. Generative Agents: Interactive Simulacra of Human Behavior. In *Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology, UIST 2023, San Francisco, CA, USA, 29 October 2023- 1 November 2023.* ACM, 2:1–2:22. https://doi.org/10.1145/3586183.3606763

[32] Lev Poretski, Joel Lanir, and Ofer Arazy. 2018. Normative Tensions in Shared Augmented Reality. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 142 (nov 2018), 22 pages. https://doi.org/10.1145/3274411

[33] Shwetha Rajaram, Chen Chen, Franziska Roesner, and Michael Nebeling. 2023. Eliciting Security & Privacy-Informed Sharing Techniques for Multi-User Augmented Reality. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, CHI 2023, Hamburg, Germany, April 23-28, 2023.* ACM, 98:1–98:17. https://doi.org/10.1145/3544548.3581089

[34] Shwetha Rajaram, Macarena Peralta, Janet G. Johnson, and Michael Nebeling. 2025. Exploring the Design Space of Privacy-Driven Adaptation Techniques for Future Augmented Reality Interfaces. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems, CHI 2025, YokohamaJapan, 26 April 2025- 1 May 2025.* ACM, 1226:1–1226:19. https://doi.org/10.1145/3706598.3713320

[35] Shwetha Rajaram, Franziska Roesner, and Michael Nebeling. 2023. Reframe: An Augmented Reality Storyboarding Tool for Character-Driven Analysis of Security & Privacy Concerns. In *Proceedings of the 36th Annual ACM Symposium on User*

Interface Software and Technology, UIST 2023, San Francisco, CA, USA, 29 October 2023- 1 November 2023, Sean Follmer, Jeff Han, Jürgen Steimle, and Nathalie Henry Riche (Eds.). ACM, 117:1–117:15. https://doi.org/10.1145/3586183.3606750

[36] Derek Reilly, Mohamad Salimian, Bonnie MacKay, Niels Mathiasen, W. Keith Edwards, and Juliano Franz. 2014. SecSpace: prototyping usable privacy and security for mixed reality collaborative environments. In *Proceedings of the 2014 ACM SIGCHI Symposium on Engineering Interactive Computing Systems* (Rome, Italy) *(EICS '14)*. Association for Computing Machinery, New York, NY, USA, 273–282. https://doi.org/10.1145/2607023.2607039

[37] Franziska Roesner, Tadayoshi Kohno, and David Molnar. 2014. Security and privacy for augmented reality systems. *Commun. ACM* 57, 4 (2014), 88–96. https://doi.org/10.1145/2580723.2580730

[38] Franziska Roesner, Tadayoshi Kohno, Alexander Moshchuk, Bryan Parno, Helen J. Wang, and Crispin Cowan. 2012. User-Driven Access Control: Rethinking Permission Granting in Modern Operating Systems. In *IEEE Symposium on Security and Privacy, SP 2012, 21-23 May 2012, San Francisco, California, USA*. IEEE Computer Society, 224–238. https://doi.org/10.1109/SP.2012.24

[39] Franziska Roesner, David Molnar, Alexander Moshchuk, Tadayoshi Kohno, and Helen J. Wang. 2014. World-Driven Access Control for Continuous Sensing. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3-7, 2014*. ACM, New York, NY, USA, 1169–1181. https://doi.org/10.1145/2660267.2660319

[40] Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2019. Secure Multi-User Content Sharing for Augmented Reality Applications. In *28th USENIX Security Symposium, USENIX Security 2019, Santa Clara, CA, USA, August 14-16, 2019*. USENIX Association, Berkeley, CA, USA, 141–158. https://www.usenix.org/conference/usenixsecurity19/presentation/ruth

[41] Antti Salovaara and Leevi Vahvelainen. 2025. Triangulating on Possible Futures: Conducting User Studies on Several Futures Instead of Only One. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems, CHI 2025, YokohamaJapan, 26 April 2025- 1 May 2025*. ACM, 478:1–478:16. https://doi.org/10.1145/3706598.3713565

[42] Florian Schaub, Bastian Könings, and Michael Weber. 2015. Context-Adaptive Privacy: Leveraging Context Awareness to Support Privacy Decision Making. *IEEE Pervasive Comput.* 14, 1 (2015), 34–43. https://doi.org/10.1109/MPRV.2015.5

[43] Florian Schaub, Peter Lang, Bastian Könings, and Michael Weber. 2013. PriCal: dynamic privacy adaptation of collaborative calendar displays. In *The 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing, UbiComp '13, Zurich, Switzerland, September 8-12, 2013 - Adjunct Publication*. ACM, 223–226. https://doi.org/10.1145/2494091.2494163

[44] Raymond Scupin. 1997. The KJ Method: A Technique for Analyzing Data Derived from Japanese Ethnology. *Human Organization* 56, 2 (1997), 233–237.

[45] Zixiong Su, Shitao Fang, and Jun Rekimoto. 2023. LipLearner: Customizable Silent Speech Interactions on Mobile Devices. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, CHI 2023, Hamburg, Germany, April 23-28, 2023*. ACM, 696:1–696:21. https://doi.org/10.1145/3544548.3581465

[46] Kentaro Taninaka, Rahul Jain, Jingyu Shi, Kazunori Takashio, and Karthik Ramani. 2025. Transparent Barriers: Natural Language Access Control Policies for XR-Enhanced Everyday Objects. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems, CHI 2025, YokohamaJapan, 26 April 2025- 1 May 2025*. ACM, 630:1–630:20. https://doi.org/10.1145/3706598.3713656

[47] Xuhai Xu, Anna Yu, Tanya R. Jonker, Kashyap Todi, Feiyu Lu, Xun Qian, João Marcelo Evangelista Belo, Tianyi Wang, Michelle Li, Aran Mun, Te-Yen Wu, Junxiao Shen, Ting Zhang, Narine Kokhlikyan, Fulton Wang, Paul Sorenson, Sophie Kahyun Kim, and Hrvoje Benko. 2023. XAIR: A Framework of Explainable AI in Augmented Reality. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, CHI 2023, Hamburg, Germany, April 23-28, 2023*. ACM, 202:1–202:30. https://doi.org/10.1145/3544548.3581500

[48] Yaqing Yang, Tony W. Li, and Haojian Jin. 2024. On the Feasibility of Predicting Users' Privacy Concerns using Contextual Labels and Personal Preferences. In *Proceedings of the CHI Conference on Human Factors in Computing Systems, CHI 2024, Honolulu, HI, USA, May 11-16, 2024*. ACM, 792:1–792:20. https://doi.org/10.1145/3613904.3642500

[49] Shaohu Zhang, Zhouyu Li, and Anupam Das. 2023. VoicePM: A Robust Privacy Measurement on Voice Anonymity. In *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2023, Guildford, United Kingdom, 29 May 2023 - 1 June 2023*. ACM, 215–226. https://doi.org/10.1145/3558482.3590175

A Appendix

A.1 Equilibrium Optimization Algorithms

Algorithm 1 presents pseudo-code for solving the Privacy-First optimization objective, as detailed in Section 4.6.

Algorithm 1 Privacy-First Optimization Pseudo-Code

Inputs: AR Sensing Profiles $\{s_{ij}\}$, Interpersonal Privacy Profiles $\{p_{ij}\}$, Permission Satisfaction thresholds $\{\mathcal{S}_i\}$, Privacy Satisfaction thresholds $\{\mathcal{P}_i\}$, function weights $\{w_{ij}\}$, where i indexes users and j indexes sensing functions
Output: Negotiated permissions $\{x_j\}$
Variables: Permission Satisfaction Score before (after) change S_{ij} (S'_{ij}), Privacy Satisfaction Score before (after) change P_{ij} (P'_{ij}), sensing function to loosen j^*

```
for each sensing function $j$ do
    $x_j \leftarrow \max_i\{p_{ij}\}$        ▷ Initialize negotiated sensing configuration to most restrictive for max privacy
end for
while $\{\mathcal{S}_i\}$ and $\{\mathcal{P}_i\}$ thresholds not met do        ▷ Loop while Permission and Privacy Satisfaction thresholds are not met
    for each sensing function $j$ do
        $\Delta S_{ij} \leftarrow \min_i S_{ij} - \min_i S'_{ij}$        ▷ Compute difference in Permission Satisfaction Score if sensing function $j$ loosened
        $\Delta Pij \leftarrow \min_i P'_{ij} - \min_i P_{ij}$        ▷ Compute difference in Privacy Satisfaction Score if sensing function $j$ loosened
        tradeoffScore $\leftarrow \frac{\Delta S_{ij}}{1+\Delta Pij}$
        if tradeoffScore > bestTradeoffScore then
            $j^* \leftarrow j$
            bestTradeoffScore $\leftarrow$ tradeoffScore        ▷ Maximize Permission Satisfaction with minimal Privacy Satisfaction loss
        end if
    end for
    $x_{j^*} \leftarrow x_{j^*} + 1$        ▷ Loosen sensing function that achieves the best tradeoff
end while
```

The Interaction-First strategy can be written as:

$$\max_{x_j} \min_{i} \quad \sum_j w_{ij} P_{ij} \tag{6}$$

$$\text{subject to} \quad \sum_j S_{ij} \geq \mathcal{S}_i, \quad \forall i \tag{7}$$

$$(1), (2)$$

$$x_j, s_{ij}, p_{ij} \in \{0, 1, \ldots, N\}$$

It guarantees that every user meets their Permission Satisfaction threshold $\mathcal{S}_i$, and seeks to meet their Privacy Satisfaction thresholds by maximizing the minimum Privacy Satisfaction Score across all users.

A.2 AR Sensing Profile Format and Example

For reference, we include the AR Sensing Profile format from our Unity implementation, defined as a C# class. To simulate fine-grained sensing negotiations, we designed a permission model in-line with recent work [24], stratifying permissions across sensing capabilities (e.g., spatial mapping) with different access levels for three data operations: capturing, computing, and storing sensor data. Each data operation is assigned a Permission Priority (*Must Have*, *Nice To Have*, and *Can Do Without*) to indicate the importance of each sensing function to app functionality. These priority values serve as weights in calculating the Permission and Privacy Satisfaction Scores (Sec. 4.6).

```
public class ARSensingProfile {
    public SensingPermissions SpatialMapping;
    public SensingPermissions GestureRecognition;
    public SensingPermissions SpeechRecognition;
    public SensingPermissions EyeTracking;
    public SensingPermissions Gaze;
    public SensingPermissions ObjectDetection;
    public SensingPermissions PeopleDetection;
}
public class SensingPermissions {
    public CapturePermissions Capture;
    public PermissionPriority CapturePriority;
    public string CaptureRationale;

    public ComputationPermissions Computation;
    public PermissionPriority ComputationPriority;
    public string ComputationRationale;

    public StoragePermissions Storage;
    public PermissionPriority StoragePriority;
    public string StorageRationale;
}
public enum CapturePermissions { Live, Precaptured, None }
public enum ComputationPermissions { CloudAndLocal, Local, None }
public enum StoragePermissions { CloudAndLocal, Local, None }
public enum PermissionPriority { MustHave, NiceToHave, CanDoWithout }
```

A.2.1 Example App Sensing Profile: Accessible Navigation. Our toolkit includes five initial AR Sensing Profiles in JSON format, corresponding to *Accessible Navigation*, *Messaging*, *Telepresence*, and *Virtual Desktop* applications, along with a generic profile that requests no permissions to represent non-AR users (*NotUsingAR*). We generated these profiles by prompting GPT-4o with descriptions of each application and the corresponding JSON structure, then manually refining them for accuracy and specificity. New profiles can be defined through JSON files placed in the /Resource directory in the Unity Assets folder. These profiles are converted to an `ARSensingProfile` C# class at runtime.

Here, we show the full profile for the Accessible Navigation application used in our hospital scenario (Sec. 6.1). Additional predefined profiles in our toolkit are provided in the Supplementary Material.

```
{ "Name": "Accessible Navigation",
  "Permissions": {
    "SpatialMapping": {
      "Capture": "Live",
      "CapturePriority": "MustHave",
      "CaptureRationale": "Real-time spatial mapping is necessary for detecting obstacles and creating safe walking paths.",
      "Computation": "Local",
      "ComputationPriority": "MustHave",
      "ComputationRationale": "Local computation ensures timely processing of spatial data for real-time navigation feedback.",
      "Storage": "None",
      "StoragePriority": "CanDoWithout",
      "StorageRationale": "Persistent storage is not required as spatial mapping is only relevant for immediate navigation."
    },
    "GestureRecognition": {
      "Capture": "None",
      "CapturePriority": "CanDoWithout",
      "CaptureRationale": "Gesture recognition is not critical for the app's functionality.",
      "Computation": "None",
      "ComputationPriority": "CanDoWithout",
      "ComputationRationale": Gesture-based user input is not required, since the navigation application takes speech input.",
      "Storage": "None",
      "StoragePriority": "CanDoWithout",
      "StorageRationale": "Gesture storage is not needed, as gestures can be processed in real time without being retained."
    },
    "SpeechRecognition": {
      "Capture": "Live",
      "CapturePriority": "NiceToHave",
      "CaptureRationale": "Live speech recognition can allow voice commands for navigation, but it is not strictly required.",
      "Computation": "Local",
      "ComputationPriority": "NiceToHave",
      "ComputationRationale": "Local computation ensures responsiveness for recognizing voice commands.",
      "Storage": "None",
      "StoragePriority": "CanDoWithout",
      "StorageRationale": "Speech storage is not needed, as commands can be processed in real time without being retained."
    },
    "EyeTracking": {
      "Capture": "None",
      "CapturePriority": "CanDoWithout",
      "CaptureRationale": "Eye-tracking is not required for the app's core functionality.",
      "Computation": "None",
      "ComputationPriority": "CanDoWithout",
     "ComputationRationale": "No computation for eye-tracking are necessary, as the app does not utilize eye gaze for interaction.",
      "Storage": "None",
      "StoragePriority": "CanDoWithout",
      "StorageRationale": "Eye-tracking data storage is not applicable since the app does not rely on this sensing capability."
    },
    "Gaze": {
      "Capture": "Live",
      "CapturePriority": "NiceToHave",
      "CaptureRationale": "Live gaze could enhance navigation by determining the user's head orientation to align spatial audio.",
      "Computation": "Local",
      "ComputationPriority": "NiceToHave",
      "ComputationRationale": "Local computation ensures responsive processing of gaze data without requiring cloud resources.",
      "Storage": "None",
      "StoragePriority": "CanDoWithout",
      "StorageRationale": "Gaze data storage is not needed, as it is only relevant for real-time feedback and alignment."
    },
    "ObjectDetection": {
      "Capture": "Live",
      "CapturePriority": "MustHave",
      "CaptureRationale": "Live object detection is essential for identifying obstacles and safe paths in real time.",
      "Computation": "Local",
      "ComputationPriority": "MustHave",
      "ComputationRationale": "Local computation ensures timely processing of object detection data for immediate feedback.",
      "Storage": "None",
      "StoragePriority": "CanDoWithout",
      "StorageRationale": "Persistent object detection storage is not required, as the data is only needed in real-time."
    },
    "PeopleDetection": {
      "Capture": "Live",
      "CapturePriority": "MustHave",
      "CaptureRationale": "Live people detection is critical to identify individuals and ensure safe navigation.",
      "Computation": "Local",
      "ComputationPriority": "MustHave",
      "ComputationRationale": "Local computation enables real-time processing of data, ensuring prompt feedback to the user.",
      "Storage": "None",
      "StoragePriority": "CanDoWithout",
      "StorageRationale": "Persistent storage of people detection data is not necessary, as the data is only used temporarily."
    }
  }
}
```

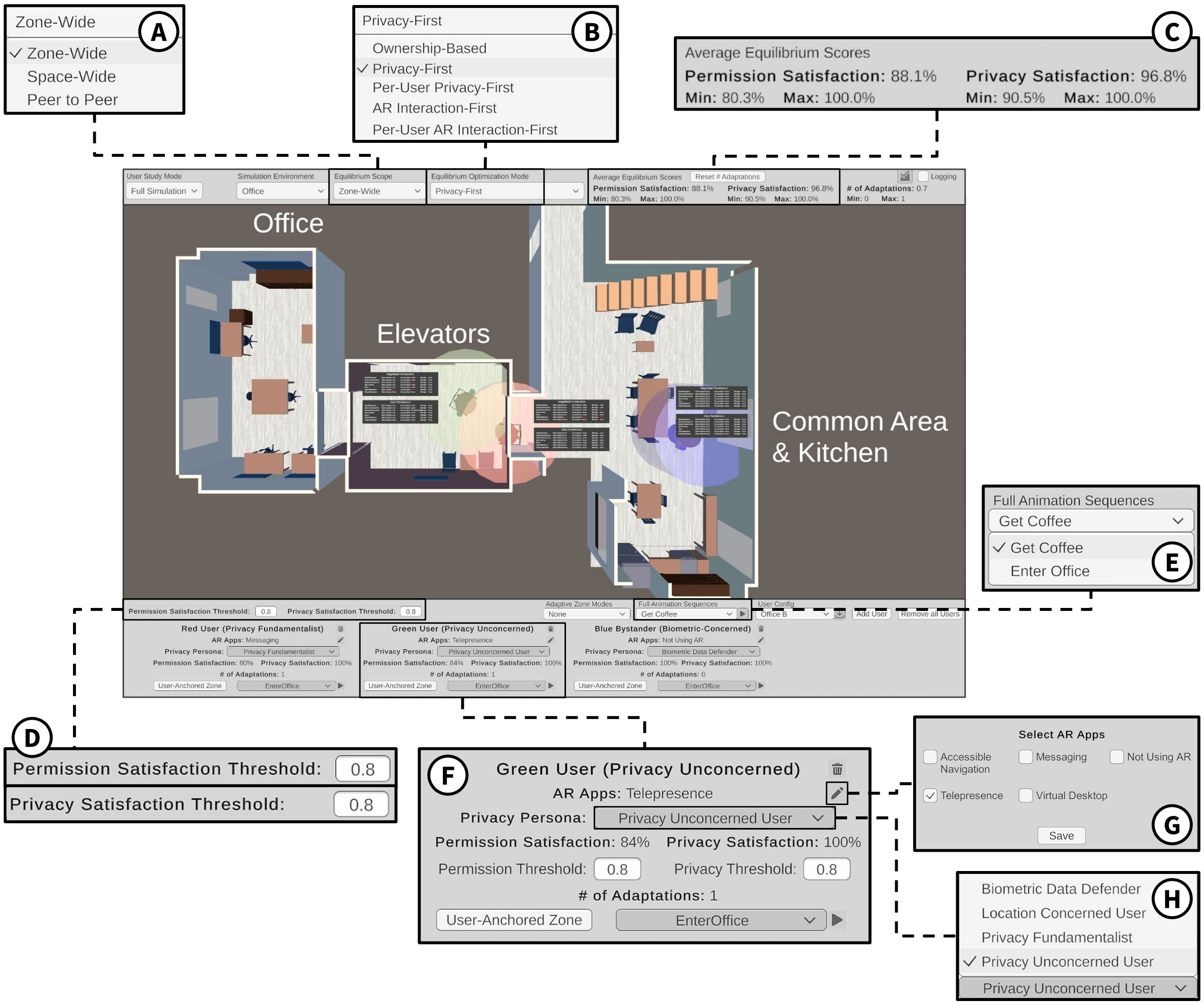
A.3 Interpersonal Privacy Profile Example

In our current implementation, Interpersonal Privacy Profiles are expressed as privacy personas [15] are mapped to a permission model in the same format as the AR Sensing Profile (Appendix A.2). Our toolkit supports flexibly adjusting the format.

We provide an example profile corresponding to a *Privacy Fundamentalist* persona who seeks to minimize other AR users’ capture and processing of data that could reveal their activities or sensitive information about them. As with the AR Sensing Profiles, we prompted GPT-4o to generate initial profiles, given descriptions of each persona as input, then we revised for accuracy and specificity. Please reference the Supplementary Material for other Interpersonal Privacy Profiles included in the toolkit (*Privacy Unconcerned User*, *Biometric Data-Concerned User*, *Location-Concerned User*).

```
{ "Name": "Privacy Fundamentalist",
  "Permissions": {
    "SpatialMapping": {
      "Capture": "Precaptured",
      "CapturePriority": "MustHave",
      "CaptureRationale": "Prefers precaptured data to reduce risk of live environmental tracking by other users.",
      "Computation": "Local",
      "ComputationPriority": "MustHave",
       "ComputationRationale": "Accepts local processing to prevent external access or remote analysis of spatial environments.",
      "Storage": "None",
      "StoragePriority": "MustHave",
      "StorageRationale": "Rejects storage to avoid future access or misuse of spatial environment data."
    },
    "GestureRecognition": {
      "Capture": "Live",
      "CapturePriority": "MustHave",
      "CaptureRationale": "Allows limited live gesture use that doesn’t reveal identity or behavioral patterns.",
      "Computation": "Local",
      "ComputationPriority": "MustHave",
     "ComputationRationale": "Requires local processing to prevent gesture data from being transmitted or analyzed externally.",
      "Storage": "None",
      "StoragePriority": "MustHave",
      "StorageRationale": "Does not allow gesture data to be stored or referenced later."
    },
    "SpeechRecognition": {
      "Capture": "Precaptured",
      "CapturePriority": "MustHave",
      "CaptureRationale": "Only comfortable with pre-recorded speech to avoid live monitoring or unintended listening.",
      "Computation": "Local",
      "ComputationPriority": "MustHave",
      "ComputationRationale": "Permits local speech processing to avoid exposing conversations to external servers.",
      "Storage": "None",
      "StoragePriority": "MustHave",
      "StorageRationale": "Rejects speech storage to prevent misuse or unauthorized review of voice content."
    },
    "EyeTracking": {
      "Capture": "Live",
      "CapturePriority": "MustHave",
      "CaptureRationale": "Permits live eye tracking only if data stays local and untraceable.",
      "Computation": "Local",
      "ComputationPriority": "MustHave",
      "ComputationRationale": "Demands local-only processing to prevent external use of sensitive eye movement patterns.",
      "Storage": "None",
      "StoragePriority": "MustHave",
      "StorageRationale": "Requires no retention of eye-tracking data to eliminate future privacy risks."
    },
    "Gaze": {
      "Capture": "Live",
      "CapturePriority": "MustHave",
      "CaptureRationale": "Live gaze tracking allowed only if data is not stored or remotely processed.",
      "Computation": "Local",
      "ComputationPriority": "MustHave",
      "ComputationRationale": "Gaze data must be processed locally to safeguard orientation-related privacy.",
      "Storage": "None",
      "StoragePriority": "MustHave",
      "StorageRationale": "No storage of gaze information to prevent profiling or retrospective inference."
    },
    "ObjectDetection": {
      "Capture": "None",
      "CapturePriority": "MustHave",
      "CaptureRationale": "Does not permit object recognition due to risks of exposing private possessions.",
      "Computation": "None",
      "ComputationPriority": "MustHave",
      "ComputationRationale": "Prohibits object analysis to avoid identifying personal belongings or contextual clues.",
      "Storage": "None",
      "StoragePriority": "MustHave",
      "StorageRationale": "Object data should never be saved to eliminate potential privacy violations."
    },
    "PeopleDetection": {
      "Capture": "None",
      "CapturePriority": "MustHave",
      "CaptureRationale": "Rejects detection of individuals to protect physical presence and personal identity.",
      "Computation": "None",
      "ComputationPriority": "MustHave",
      "ComputationRationale": "No people analysis allowed to avoid identification, profiling, or location tracking.",
      "Storage": "None",
      "StoragePriority": "MustHave",
      "StorageRationale": "People data must not be stored to preserve anonymity and privacy."
    }
  }
}
```

A.4 Unity Simulation Engine Interface Walkthrough



Average Equilibrium Scores
Permission Satisfaction: 88.1% **Privacy Satisfaction:** 96.8%
Min: 80.3% **Max:** 100.0% **Min:** 90.5% **Max:** 100.0%

Permission Satisfaction Threshold: 0.8
Privacy Satisfaction Threshold: 0.8

Green User (Privacy Unconcerned)
AR Apps: Telepresence
Privacy Persona: Privacy Unconcerned User
Permission Satisfaction: 84% Privacy Satisfaction: 100%
Permission Threshold: 0.8 Privacy Threshold: 0.8
# of Adaptations: 1

□ Accessible Navigation □ Messaging □ Not Using AR
☑ Telepresence □ Virtual Desktop

Figure 11: Simulation Engine Interface. Section 5 details our toolkit's three-step workflow for simulating multi-user scenarios and different ways to negotiate a Privacy Equilibrium. Here, we walk through how to perform each step in the simulation engine's user interface.

Step 1: Specifying the Context of Use. The bottom toolbar provides controls to add AR users and bystanders to the scene (F), then customize their AR applications (G) and privacy persona (H). Toolkit users can define new AR Sensing Profiles and Interpersonal Privacy Profiles as JSON files in the /Resource directory, using the format specified in Appendices A.2-A.3. Pre-scripted animation sequences can be triggered on a per-user basis (F) or for multiple users at a time (E) to illustrate their movements in the space. New animations can be recorded via Unity's Timeline Animation tools and linked to a particular simulation environment through an associated C# script.

Step 2: Configuring the Negotiation Process. Toolkit users can experiment with different Equilibrium Scopes (A) and Optimization Strategies (B) through dropdowns in the top toolbar. For simplicity, we separate the Privacy-First and Interaction-First strategies into two modes (B): one applies global thresholds for Permission and Privacy Satisfaction across all users (configured in D). The "Per-User" Privacy-First and Interaction-First modes allow setting individual score thresholds (F), enabling prioritization of specific users' needs, for example, assigning a higher Privacy threshold to favor the blue bystander's preferences in the Office scenario.

Step 3: Analyzing UX & Privacy Tradeoffs. To weigh the impact of negotiation strategies on all users in real time, toolkit users can monitor the Equilibrium Scores on a per-user basis (F) and as aggregated averages across all users (C).

A.5 Hospital Application Scenario: Detailed Walkthrough

In this section, we first detail how we selected threshold combinations for our application scenarios (Sec. 6) to produce distinct Equilibrium points along the Pareto Frontier. Then, we walk through the full execution of the Privacy-First algorithm for the hospital scenario (Sec. 6.1).

A.5.1 Threshold Selection Process. To systematically explore negotiation strategies enabled by our framework, we ran a series of simulations to identify Permission and Privacy Satisfaction threshold pairs that consistently yield distinct sensing configurations (i.e., Equilibrium points) across different privacy personas. First, we configured three pairs of personas with varying levels of privacy concern (combinations of *Privacy Fundamentalist*, *Unconcerned*, and *Biometric Data-Concerned* users). Then, assuming all personas were using the same AR Messaging app, we computed Privacy-First negotiations, varying both thresholds from 0.6 to 1.0 in 0.1 intervals. This setup involved 27 threshold pairs per persona combination, for a total of 81 trials.

Then, we averaged the Permission and Privacy Satisfaction Scores for each persona combination and computed a five-number summary for each. By analyzing the distance of each trial to the 1st quartile, median, and 3rd quartile, we identified the threshold combinations closest to these markers across all trials. In other words, these threshold pairs produced different Equilibrium points from one another in all three persona scenarios. Table 1 summarizes the final threshold pairs that we used in our application scenarios (Sec. 6) and toolkit walkthroughs with S&P researchers (Sec. 7).

	Privacy-First*				**Interaction-First***				**Ownership-Based***
Permission Satisfaction Threshold	0	0.8	0.6	0.7	1	0.8	0.8	0.9	–
Privacy Satisfaction Threshold	1	0.8	0.8	0.9	0	0.8	0.6	0.7	–

Table 1: Threshold Combinations used in Application Scenarios. Based on our threshold selection process, we chose three pairs of Permission Satisfaction thresholds ($\mathcal{S}_i$) and Privacy Satisfaction thresholds ($\mathcal{P}_i$) that produce different Privacy Equilibrium points along the Pareto Frontier ($\{\mathcal{S}_i = 0.8, \mathcal{P}_i = 0.8\}$, $\{\mathcal{S}_i = 0.6, \mathcal{P}_i = 0.8\}$, $\{\mathcal{S}_i = 0.7, \mathcal{P}_i = 0.9\}$) for the Privacy-First strategy. For the Interaction-First strategy, we flipped the threshold values to set a higher Permission Satisfaction threshold than Privacy Satisfaction threshold (e.g., $\{\mathcal{S}_i = 0.8, \mathcal{P}_i = 0.6\}$). We added threshold pairs that completely maximize Privacy Satisfaction ($\{\mathcal{S}_i = 0, \mathcal{P}_i = 1\}$) for the Privacy-First approach and maximize Permission Satisfaction ($\{\mathcal{S}_i = 1, \mathcal{P}_i = 0\}$) for the Interaction-First approach.

(*) We simulated each Optimization Strategy with the Space-Wide and Zone-Wide scopes.

A.5.2 Walkthrough of Space-Wide, Privacy-First Optimization Algorithm. Our hospital application scenario (Sec. 6.1, Fig. 9), illustrates a Space-Wide, Privacy-First negotiation where both the low-vision user's and *Location-Concerned* bystander's thresholds for Permission Satisfaction ($\mathcal{S}_i = 0.8$) and Privacy Satisfaction ($\mathcal{P}_i = 0.8$) were already met, so all permissions were granted to the low-vision user. However, if we adjust these thresholds to $\{\mathcal{S}_i = 0.7, \mathcal{P}_i = 0.9\}$, the bystander's Privacy Satisfaction threshold is no longer met by default.

We walk through the Privacy-First algorithm (Alg. 1) for this case. Appendix A.2 includes the low-vision user's AR Sensing Profile for the Accessible Navigation app. Please find the bystander's *Location-Concerned* Interpersonal Privacy Profile in the Supplementary Material.

First Iteration of Privacy-First Optimization Algorithm. The Privacy-First approach attempts to adjust the low-vision user's AR Sensing Profile to align with the *Location-Concerned* bystander's Interpersonal Privacy Profile. (Note that the low-vision user is the only AR user in this scenario; in scenarios with multiple users, the algorithm would act on all of their AR Sensing Profiles). The algorithm starts by initializing the low-vision user's negotiated sensing configuration to the most restrictive set of permissions, as defined by the bystander's Interpersonal Privacy Profile (Table 2, Column B).

(A) Sensing Functions to Loosen	(B) Current Negotiated Value	(C) Desired Value	(D) 1st Iteration Tradeoff Scores
Spatial Mapping (Capture)	Precaptured	Live	0.0953*
Speech Recognition (Capture)	None	Live	0
People Detection (Capture)	None	Live	0
Gesture Recognition (Computation)	None	None	0
Speech Recognition (Computation)	None	Local	0.0508
People Detection (Computation)	None	Local	0.0953
Gesture Recognition (Storage)	None	None	0

Table 2: Privacy-First Algorithm's First Iteration. (*) indicates the best Permission-Privacy Satisfaction tradeoff score.

Next, we obtain a list of possible sensing functions to loosen (Table 2A). This includes all permissions that the bystander's Interpersonal Privacy Profile requests restrictions upon. The algorithm iterates through these sensing functions and first computes the change in both users' Permission and Privacy Satisfaction Scores if we were to loosen this function. If no user's Privacy Satisfaction threshold would be violated, we calculate a tradeoff score (Table 2D), defined as $\left(\max \frac{\Delta S_i}{1+\Delta P_i}\right)$. In other words, the highest tradeoff score achieves the greatest gain in Permission Satisfaction while minimizing loss in Privacy Satisfaction.

In this case, loosening the negotiated value for Spatial Mapping Capture (from *Precaptured* to *Live*) produced the best tradeoff score (indicated by * in Column D), as did loosening People Detection Computation later in the loop. Four sensing functions achieved a tradeoff score of 0. In the case of Speech Recognition Capture and People Detection Capture, this is because granting one level of access higher from *None* would still not achieve the desired value of *Live*. In the case of Gesture Recognition (Computation and Storage), the low-vision user does not require access to these capabilities, so there would be no Permission Satisfaction gain.

At this point, the algorithm chooses Spatial Mapping Capture as the best sensing function to loosen, changing its value from *Precaptured* to *Live*.

Second Iteration of Privacy-First Optimization Algorithm. The algorithm follows the same procedure as the first iteration to evaluate tradeoffs with loosening each sensing function (summarized in Table 3). The function we loosened in the first iteration, Spatial Mapping Capture, already meets the low-vision user's desired value. Of the remaining sensing functions, only Speech Recognition Computation is viable to loosen. This is because loosening the other permissions would either not raise the low-vision user's Permission Satisfaction Score or would lower the bystander's Privacy Satisfaction Score beyond their threshold ($\mathcal{P}_i = 0.9$).

(A) Sensing Functions to Loosen	**(B) Current Value**	**(C) Desired Value**	**(D) 1st Iteration Tradeoff Scores**
Spatial Mapping (Capture)	Live	Live	*already at desired value*
Speech Recognition (Capture)	None	Live	0
People Detection (Capture)	None	Live	0
Gesture Recognition (Computation)	None	None	0
Speech Recognition (Computation)	None	Local	0.0508*
People Detection (Computation)	None	Local	*loosening would violate bystander's Privacy threshold*
Gesture Recognition (Storage)	None	None	0

Table 3: Privacy-First Algorithm's Second Iteration. (*) indicates the best Permission-Privacy Satisfaction tradeoff score.

As it is not possible to loosen any other sensing functions and achieve a non-zero tradeoff score, the algorithm loosens Speech Recognition Computation from *None* to *Local* and returns. We note that for simplicity in this example, we calculate the Permission Satisfaction Score as a binary value per sensing function: 1 if the current value equals the desired value; 0 otherwise (Eqn. 1). With a less stringent calculation for Permission Satisfaction Score that takes into account how "close" each sensing function's current value is to the desired value ($0 < S_{ij} < 1$), the algorithm would try adjusting other sensing functions that need to be loosened multiple times to meet the desired value (i.e., Speech Recognition Capture and People Detection Capture).