OurData: Understanding Family Privacy in Sensor-Rich Homes

HYUNSOO LEE*, KAIST, Republic of Korea
REZA GHAIUMY ANARAKY, Louisiana State University, United States
ODED NOV, New York University, United States
UICHIN LEE, KAIST, Republic of Korea

The rise of IoT devices in domestic and shared home environments produces interpersonal data that implicates multiple family members, giving rise to privacy concerns that individual control alone cannot adequately address. We conducted vignette-based interviews with 10 families (N = 34) to examine how household members experience and negotiate sensing technologies in everyday family life. Participants understood family data not merely as aggregated personal data, but as a socially embedded and relationally meaningful form shaped by shared routines, roles, and caregiving practices. We present *OurData* as an analytical lens that emerged from these findings to capture how sensing data in family contexts is collectively produced, interpreted through relationships, and ethically implicated across household members. We further offer design guidance for ubiquitous sensing systems that support family privacy through relational accountability, interpersonal awareness, and context-sensitive negotiation of shared data.

CCS Concepts: • **Security and privacy** → **Social aspects of security and privacy**; • **Human-centered computing** → **Social content sharing**; **HCI theory, concepts and models**.

Additional Key Words and Phrases: smarthome, privacy

ACM Reference Format:
Hyunsoo Lee, Reza Ghaiumy Anaraky, Oded Nov, and Uichin Lee. 2026. OurData: Understanding Family Privacy in Sensor-Rich Homes. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 10, 2, Article 50 (June 2026), 27 pages. https://doi.org/10.1145/3810233

1 INTRODUCTION

The proliferation of IoT devices and sensor technologies has enabled the collection of detailed records of everyday activities. Although these technologies are often designed with individual users in mind, the data they generate frequently implicate multiple people and require collective interpretation. Research in ubiquitous computing has increasingly examined group-based and interpersonal data, showing how shared sensing environments give rise to collective privacy concerns and interdependent risks [16, 29, 32]. Studies of family exergames [64], shared mental health displays [41], and workplace sensing [3] demonstrate that data are co-produced through social interaction and acquire meaning at the group level, rather than being attributable to a single individual [32].

These dynamics are particularly salient in domestic sensing environments, where devices are embedded into everyday routines and relationships, producing data that is intertwined with family life and shaped by long-term interdependence [16, 29, 32, 33]. Prior research on smart homes and family privacy has documented challenges such as shared exposure, relational inference, and asymmetric control among household members [29, 32, 38]. From the perspective of the *semantic tangle* [35], meaning in these environments emerges from the interaction of

Authors' Contact Information: Hyunsoo Lee (corresponding author), KAIST, Daejeon, Republic of Korea, hslee90@kaist.ac.kr; Reza Ghaiumy Anaraky, Louisiana State University, Louisiana, United States, rganaraky@lsu.edu; Oded Nov, New York University, New York, United States, onov@nyu.edu; Uichin Lee, KAIST, Daejeon, Republic of Korea, uclee@kaist.edu.

ACM 2474-9567/2026/6-ART50
https://doi.org/10.1145/3810233

people, events, and spaces. This view echoes early UbiComp metaphors such as "living in a glass house," which underscore how pervasive sensing renders ordinary life increasingly observable [6, 13].

Despite these insights, much of the privacy discourse surrounding sensing technologies continues to rely on individual-centric models that assume privacy decisions can be made through explicit consent and clearly defined rule. In family smart homes, however, privacy is rarely negotiated in this way. Instead, it emerges through ongoing relationships, shared routines, and implicit expectations among household members.

However, comparatively less attention has been paid to how people themselves come to recognize sensing data as collectively relevant in everyday family life, and how such interpretations shape privacy reasoning before questions of ownership, control, or consent are articulated. In family contexts, sensing data is often difficult to decompose into individual contributions, yet prevailing analytical perspectives in prior work on group data in law, psychology, and social sciences continue to emphasize individual ownership or access rights [49, 65]. This mismatch raises fundamental questions about how privacy should be understood and designed for shared sensing environments, where data becomes meaningful through family relationships rather than individual decisions.

Motivated by this gap, our study examines how people understand and reason about the data produced in sensor-based environments shared by multiple family members. While privacy is often conceptualized as a matter of explicit consent or formal rules, our study examines how privacy meanings instead emerge through ongoing relationships, shared routines, and implicit expectations in everyday family life. We focus on family households as a primary empirical context for examining privacy in smart sensing environments. Rather than treating families as representative of all possible groups, we position them as a socially intimate and analytically rich setting in which shared data is continuously produced through everyday routines, and where privacy judgments are shaped by long-term cohabitation and unequal authority (e.g., between parents and children). This focus allows us to examine how privacy meanings emerge under conditions of continuous ambient sensing without presuming a particular model of group governance in advance. Thus, we set out the following research questions:

- RQ1: How do people make sense of and construct meanings around data produced in sensor-based environments shared by multiple family members?
- RQ2: What kinds of privacy concerns and expectations emerge in these shared sensing contexts, and how are they shaped by family relationships, roles, and everyday practices?

We conducted a qualitative study with 10 families (N = 34) using speculative vignettes grounded in real-world sensing interactions. Participants frequently interpreted the sensing data as "about us," implicating multiple family members regardless of who technically generated or controlled it. In this sense, sensing data functioned as a medium through which family boundaries, responsibilities, and moral expectations were negotiated. Based on these findings, we introduce the concept of *OurData* as an analytic lens for examining how sensing data comes to be understood as collectively meaningful and privacy-relevant in family smart homes. Rather than presuming shared data as a predefined category, *OurData* captures how collectivity and privacy concerns emerge through everyday encounters with sensing technologies, before questions of individual ownership, control, or consent are articulated. The contributions of this study are threefold:

- We provide an empirical analysis of how family members interpret sensing data as collectively implicated, introducing *OurData* as an analytic concept for this relational orientation toward shared data.
- We offer empirical insights into family privacy in smart homes by showing how concerns such as shared exposure, relational inference, surveillance, and asymmetric control emerge through everyday sensemaking.
- We derive design implications for smart home systems that support shared data practices, emphasizing relational and context-sensitive approaches beyond individual consent and static access control.

2 RELATED WORK

2.1 From Individual Rights to Group Privacy: Rethinking Privacy as Collective Norm

Data generated through shared devices and social interactions often captures not only individual behaviors but also shared routines and social dynamics [1, 8, 16]. These relational forms of data challenge individual-centric models of privacy, which assume ownership and control reside with a single person. The emerging discourse on *group privacy* frames data as a social artifact produced through participation, cohabitation, and interpersonal relationships [7, 70].

Even before the emergence of ubiquitous computing, the notion of group privacy has long been explored across law, psychology, and social science, where scholars have debated whether group privacy is a workable concept, especially when collective interests cannot be reduced to the rights of individual members [70]. Recent theoretical work has expanded the conceptualization of group privacy, including frameworks for understanding dependencies and interrelations among members' data [7]. While early discussions in privacy literature often treated group concerns as extensions of individual rights such as freedom of association or protections within family structures, recent studies argue that this is insufficient [49]. Group privacy is not merely the sum of individual claims, but concerns aspects such as collective identity, internal group dynamics, and shared contextual meaning. Concepts like relational or family privacy recognize that one person's data may implicate others [71], yet these protections usually rely on individual rights rather than a group's autonomous ability to protect shared data or boundaries [63].

Legal frameworks like the GDPR and CCPA partially ackowledge group concerns by safeguarding "special categories" of data (e.g., race, religion, political views), which often apply to groups [70], but group privacy is not formally recognized as a standalone right. This raises questions about defining collective data, assessing privacy risks from multi-person patterns, and establishing strategies for collective governance.

As human-data interactions increasingly permeate social contexts, computing research has developed frameworks to address collective privacy. Examples include *collective privacy* for collaborative OSN (Online Social Network) content management [69], *multi-party privacy* for conflicting OSN settings [72], *networked privacy* for effects of one person's data on others [10], *interdependent privacy* for actions affecting others through third-party apps [9], and *peer privacy* for private disclosures in peer groups [85]. One person's data decision may inadvertently affect others, complicating notions of informed consent [63].

2.2 Group Privacy in Sensing Environments

Recent advances in Internet of Things (IoT) and pervasive sensing have shown the latest evolution of Weiser's vision of ubiquitous computing, where computing becomes embedded in the fabric of everyday life and disappears into the background [75]. Even mundane objects (e.g., TV, vacuum, smart toys) have become sensor-augmented devices that continuously collect data, often without explicit user intervention, creating complex data flows implicating multiple people.

In response to this shift, researchers have discussed how pervasive computing complicates the boundaries between personal and collective data [15, 17, 29, 32]. Crabtree and Mortier [16] argue that much of the personal data we generate is co-produced through interaction, emerging not as "mine" but as "ours." Goulden et al. [32] introduced the concept of *interpersonal data* to describe data generated through shared interactions among groups, particularly in contexts like the smart home. Interpersonal data is inherently relational: it arises from collective action, affects multiple people, and resists being cleanly owned or managed by a single individual.

As devices increasingly sense and transmit data automatically, questions around consent, transparency, and ownership become more complex [15, 17, 29]. This perspective calls for data governance models that reflect the collaborative and negotiated nature of data, especially in settings with multiple people, such as homes, workplaces, and public spaces. Subsequent work highlights issues like asymmetrical visibility, ambiguous consent boundaries,

and potential collective harm when multiple parties are implicated in the same data traces [19, 60, 67, 81]. Despite these insights, most research remains theoretical, with limited empirical studies examining how people perceive, interpret, and negotiate relational, socially embedded data.

2.3 Multi-user Privacy Challenges in Smart Homes with Families

Building on these findings, family households provide a particularly relevant context for studying multi-user privacy in practice. In ubiquitous computing environments, smart home technologies continuously collect data that is often relational, ambient, and temporally extended, embedding sensors into everyday family life [34, 50, 84]. In such contexts, privacy risks are not confined to individuals, but emerge from the interdependent interactions among household members. This highlights a key limitation of individual-centric privacy models, which cannot fully capture relational dynamics in domestic environments.

Empirical studies in family households have documented specific multi-user privacy challenges. Unequal control over devices is a common concern: household members who set up and manage smart home systems—typically the more tech-savvy—often have broader access to device settings and activity logs, while other members may have limited awareness or agency [29, 38, 47, 82]. Such asymmetries shape divergent privacy experiences and, in extreme cases, can facilitate intimate partner violence or abuse [54].

Closely related to control, unintended data exposure arises as smart speakers, cameras, or activity monitors reveal behaviors, preferences, or routines to other family members or external actors [14, 45, 83, 84]. These exposures can create conflicts over routine household activities, including children's device use, shared media habits, or parental monitoring, reflecting relational privacy challenges unique to family life [30, 38, 74].

While these studies provide valuable observations, they rarely examine household-level or relational risks in a systematic way, nor do they explore how family members interpret, negotiate, and collectively manage shared data flows. In other words, prior work largely focuses on access, control, and conflict resolution, but does not capture the everyday sensemaking and relational dynamics that emerge in smart sensing environments. This gap underscores the need for conceptual approaches that explicitly consider family-specific privacy dynamics in ubiquitous computing contexts, including how household members perceive, interpret, and make sense of data generated by multiple people in real-world sensing environments.

These challenges are further compounded by the legal context. Although EU data protection law generally exempts purely personal or household activities from formal responsibility, the increasingly networked nature of smart homes blurs these boundaries, requiring families to coordinate internal responsibilities, negotiate visibility, and manage shared accountability [29]. The combination of relational, technical, and legal complexities demonstrates why family households are a critical site for studying multi-user privacy in ubiquitous computing environments.

3 METHOD

We conducted a vignette-based interview study to explore how families make sense of shared sensor data and negotiate privacy in everyday contexts. The study was designed to examine how privacy reasoning emerges around family-based sensing, rather than to evaluate specific technologies or compare use cases.

3.1 Participants

Ten families (N = 34) in Korea were recruited through school-affiliated educational institutions, which resulted in a participant pool consisting largely of households with school-aged children. All participating families had at least one school-aged child. Children younger than approximately 10 years old were excluded due to concerns about their ability to meaningfully engage in discussions.

Table 1. Participant Families and Reported Smart Device Usage.

Demographics	Reported Use of Smart Sensing Devices
Family 1 (F, M, G-13, B-12)	Wearable devices, Smart speaker, Smart camera, Smart appliances (vacuum, fridge)
Family 2 (F, M, B1-13, B2-10)	Wearable devices, Smart speaker, Smart camera, Smart appliances (vacuum, fridge), Smart sensors (lighting, humidity, door, motion)
Family 3 (F, M, B-13)	Wearable devices, Smart speaker
Family 4 (F, M, B-10)	Wearable devices, Smart speaker, Smart sensors (lighting, humidity)
Family 5 (F, M, B-12)	Wearable devices, Smart speaker, Smart camera, Smart appliances (vacuum, fridge)
Family 6 (F, M, G1-14, G2-12)	Wearable devices, Smart speaker, Smart camera, Smart sensors (lighting, sleep), Smart appliances (vacumm)
Family 7 (F, M, B-13)	Wearable devices, Smart speaker, Smart camera, Smart appliances (vacuum)
Family 8 (F, M, G1-14, G2-11)	Wearable devices, Smart speaker, Smart camera
Family 9 (F, M, G-13)	Wearable devices, Smart speaker, Smart camera, Smart sensors (lighting)
Family 10 (F, M, B-12)	Wearable devices, Smart speaker, Smart camera

Only families with prior experience using smart home or IoT devices (e.g., smart speakers, security cameras, health trackers) were eligible to participate. During sign-up, participants were asked to list all smart home devices they had used to help contextualize their familiarity with sensor-based technologies.

Families received approximately 80 USD as compensation. All procedures were IRB-approved. Written informed consent was obtained from all adult participants, and explicit assent was obtained from all children. For in-person sessions, consent was obtained on-site; for remote sessions, consent forms were explained verbally and returned by email. Participation was voluntary for all family members.

3.2 Vignette Design

We developed three independent vignettes representing everyday family contexts involving shared sensing: (1) family health management and monitoring, (2) device sharing, and (3) home monitoring and safety. These contexts are well established in prior ubiquitous computing research on smart homes and family technologies, including studies of family health monitoring and care practices [41, 45, 64], shared and multi-user devices in domestic settings [30, 32, 38, 40, 56], and home monitoring systems related to safety and surveillance [16, 29, 77]. Rather than exhaustively covering smart sensing use cases, we designed the vignettes as analytical probes that draw on familiar sensing scenarios to elicit reflection on how family privacy concerns arise as data are co-produced, accessed, and interpreted in domestic environments.

3.2.1 Design Principles and Analytic Dimensions. Building on these established sensing contexts, the three vignettes were selected to systematically vary key dimensions relevant to family privacy in sensing environments.

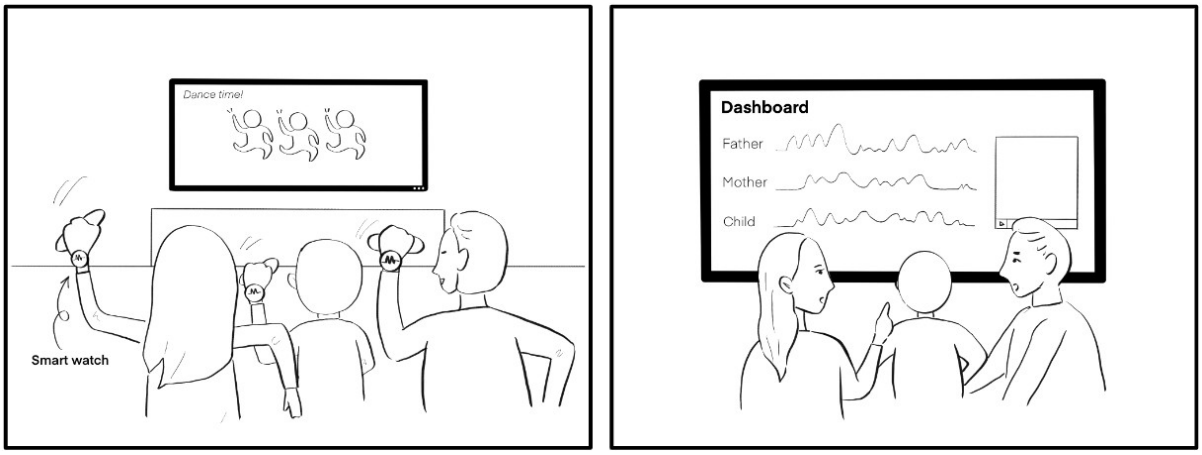

Fig. 1. Vignette 1: Family Health Management & Monitoring: A family uses smartphones and smartwatches to track and share both physical and mental health. Data includes steps, sleep, heart rate, and self-reported mood via surveys

These dimensions were drawn from recurring themes in prior smart home and family privacy literature and served as sensitizing concepts rather than a prescriptive design model.

(1) **Spatial scope of sensing** (shared domestic spaces vs. localized activities),
(2) **Temporal persistence of sensed data** (momentary capture vs. longitudinal accumulation),
(3) **Visibility and inferability of sensing outputs** (directly observable vs. inferred/derived),
(4) **Alignment or misalignment between data producers, subjects, and stakeholders**, and
(5) **Sensing modalities involved**, which shape the types of behavioral and relational inferences that can be drawn.

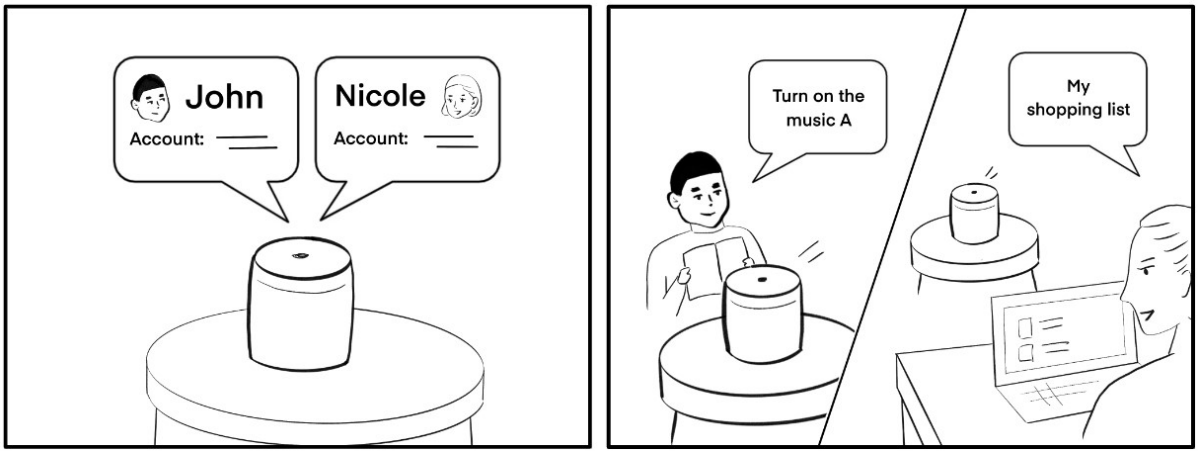

Fig. 2. Vignette 2. Device Sharing: A family uses a smart speaker linked to the husband's account for shared tasks like music, shopping, and controlling home devices. Visiting relatives occasionally use the device as well.

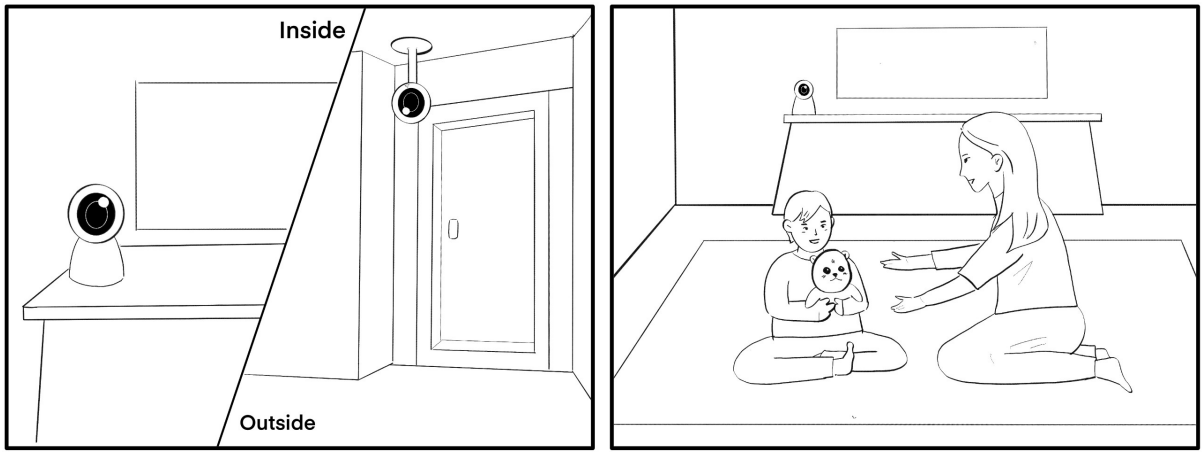

Fig. 3. Vignette 3. Home Monitoring & Safety:A family installs smart cameras inside and outside the home for safety, and uses a teddy bear-shaped smart toy with a microphone to monitor their child.

To keep the vignettes legible and grounded in participants' everyday understanding, we focused on physiological, health-related, and audio or video sensing, and intentionally excluded less visible signals such as electricity usage or network traffic. Each vignette foregrounded different aspects of these dimensions, with particular analytic emphasis. The Family Health Management vignette primarily highlighted issues related to temporal persistence and the visibility of health data; the Device Sharing vignette drew attention to misalignments between data producers, subjects, and stakeholders; and the Home Monitoring vignette emphasized questions of spatial scope and sensing modality. Across all three vignettes, however, multiple dimensions often co-occurred and interacted, reflecting the layered nature of privacy concerns in family sensing environments.

3.2.2 Ordering and Independent Design. Each vignette was treated as a standalone prompt, and participants encountered all three vignettes in a fixed order. The analysis focused on themes that cut across vignettes rather than comparing responses between them, minimizing carryover effects and avoiding narrative escalation that could bias privacy reasoning.

3.3 Storyboard-based prototype

Each vignette was paired with a lo-fi storyboard-style prototype simulating a smart home data management interface (Figure 4). While the vignettes varied everyday contexts of shared sensing, the storyboards foregrounded privacy management factors within each context.

The storyboard design was informed by prior work on privacy management at the level of sensitizing concepts, such as awareness (who can see what data) and control (who can modify, delete, or share data), and boundary negotitation [4]. These concepts were not introduced to participants as analytic categories, nor were participants asked to evaluate the scenarios using privacy management terminology. Instead, the storyboards were designed to make privacy-relevant tensions perceptible while leaving interpretation and evaluation open to participants.

This separation allowed the study to vary context through the vignettes and privacy-relevant conditions through the storyboards, supporting examination of how families reason about group privacy beyond individual-based privacy management models.

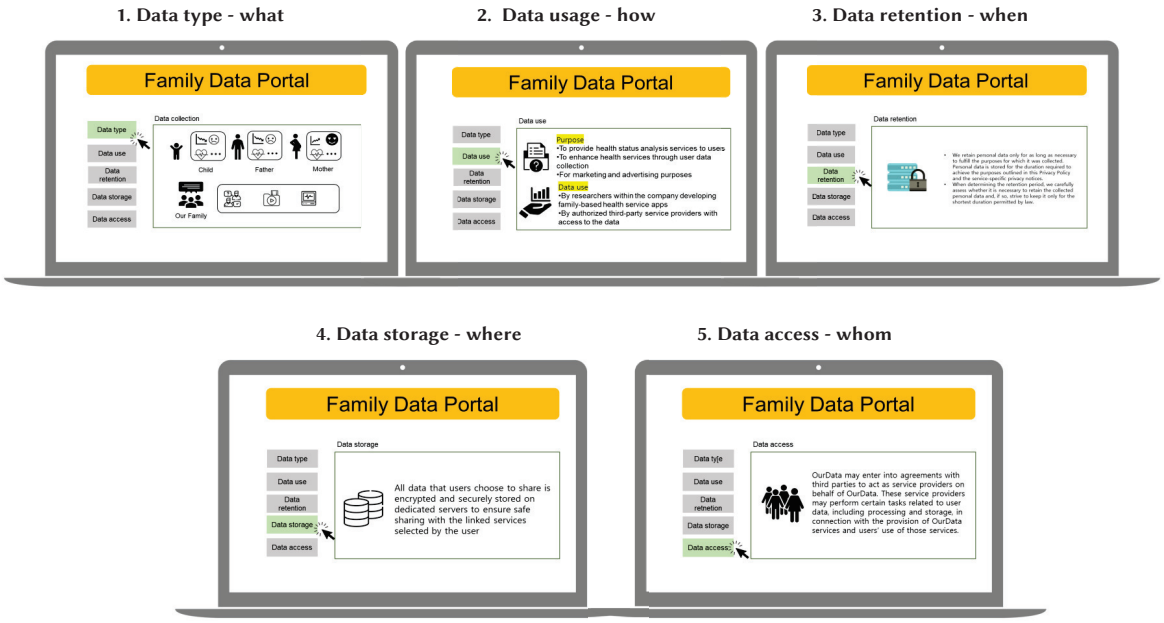

Fig. 4. Lo-Fi Storyboard Prototype.

3.4 Procedure

Before the interviews, participants were briefed on the study's purpose, procedures, and data confidentiality. Families were introduced to the context of shared sensing and general concepts of collective or family-level data without providing a fixed definition of "OurData," minimizing researcher-directed priming. Interviews were semi-structured and conversational, lasting approximately 70 minutes. Sessions were conducted in a one-family–two-interviewer format. Two interviews were conducted in person, while the remaining interviews were conducted remotely via Zoom. All interviews were conducted in Korean, the participants' native language.

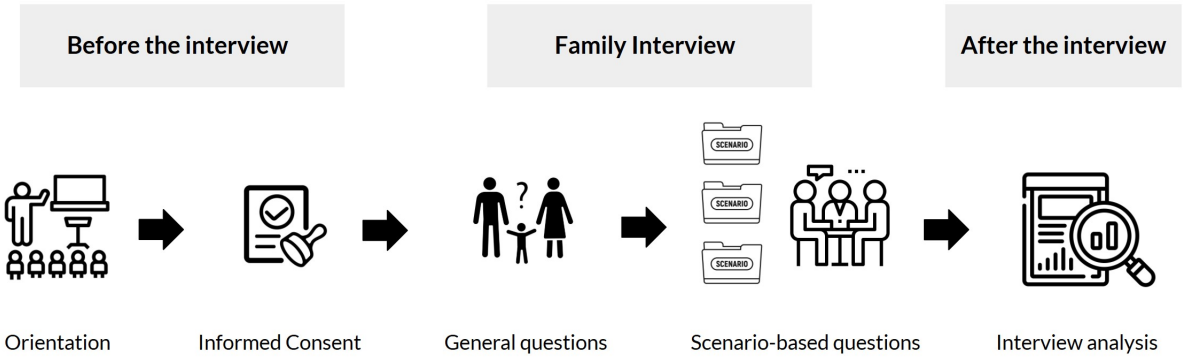

Fig. 5. Study design and procedure for the conceptualization of OurData

Facilitators maintained neutrality, encouraged elaboration, and prompted children to respond first to mitigate potential power imbalances.

3.4.1 Conceptual Framing. At the start of each session, participants were introduced to each vignette along with initial prompts aimed at eliciting their understanding of collective data. Participants reflected on shared versus personal data using their own descriptors (e.g., "jointly generated," "visible to all," or "used collectively"), enabling examination of how sensing technologies shape social and ethical experiences. These reflections informed a later typology synthesizing classification strategies across spatial, temporal, activity, and device contexts.

3.4.2 Vignette Reflection. Families engaged with all three scenarios individually. The fixed vignette order followed design workbook methodologies [18, 76, 78], emphasizing exploratory reflection rather than experimental manipulation. Each vignette was paired with its storyboard prototype, and open-ended prompts (e.g., "Would you consider this data your own, someone else's, or shared?," "Who should be able to see this?," and "What privacy concerns might arise?") guided discussion. This setup supported reflection on family data practices and negotiation of privacy boundaries.

3.4.3 Data Analysis. With participants' consent, remote sessions were video-recorded and in-person sessions audio-recorded. All recordings were transcribed and analyzed using manual qualitative coding. Four researchers independently familiarized themselves with transcripts, generated initial codes, and collaboratively refined patterns through iterative discussion. We applied *reflexive thematic analysis*, allowing codes and themes to emerge organically through interpretive engagement with participants' narratives [11], capturing both participants' conceptualization of OurData and their situated privacy reasoning in everyday family contexts.

4 RESULTS

4.1 Interpreting and Negotiating OurData in Families (RQ1)

We explored RQ1, *"How do people make sense of and construct meanings around data produced in sensor-based environments shared by multiple family members?"* Participants were encouraged to freely discuss what distinguishes personal data from group (i.e. family) data and to articulate their own understanding of what constitutes family data, including its definition, scope, and components, through concrete examples from daily life. Note that we did not predefine or introduce the term in advance. Rather than applying a predefined concept, the notion of *OurData* emerged inductively from participants' responses as they reflected on and reasoned about shared sensing data in their everyday family contexts. Our analysis proceeded in two complementary layers. First, we examined how participants conceptually articulated collectively generated data and distinguished it from personal data, drawing on classification lenses such as spatial context, relational ties, attribution, and access. Second, we examined how these conceptual understandings were enacted and refined in everyday domestic contexts through discussions grounded in the vignette scenarios, which elicited participants' situated social reasoning about shared data in relation to specific spaces, devices, activities, and family routines. While we analytically distinguish between conceptual articulation and situated reasoning, participants' articulations of OurData were often grounded in concrete examples introduced through the vignette. As a result, vignette-based references are interwoven throughout the themes reported in this section, rather than treated as a separate layer of findings (See Appendix for detailed vignette-specific participant responses)

Based on these analyses, we developed a typology, later named *OurData*, that integrates participants' reasoning across space, time, activity, and devices, bridging conceptual understanding and practical boundary negotiation. Participants are identified by family unit (P*k*) and role: Father (F), Mother (M), and Child (B: Boy, G: Girl), using the format P*k*–F/M/B/G.

Table 2. Dimensions distinguishing personal data from family data (OurData) based on participants' classification criteria. Each dimension reflects key perspectives participants used to think about data in terms of personal versus collective relevance. The "Related Themes" column indicates which thematic factors in the Results section primarily involve each dimension (i.e., T1. Shared activities in time and space, T2. Social intimacy level, T3. Individual attribution and contribution, T4. Use purpose and context, and T5. Technical definitions and data accessibility). These dimensions are not mutually exclusive but often overlap in participants' reasoning across different contexts.

Dimension	Personal Data	Family Data (OurData)	Related Themes
Space	Private spaces (e.g., bedroom) – Data from personal devices used only by the individual.	Shared spaces (e.g., living room, kitchen) – Any data collected in these spaces is considered collective.	T1, T4
Time	Asynchronous (non-concurrent) – One person interacts with a device separately.	Concurrent (synchronous) – Multiple users interact or are present when data is generated.	T1
Activity	Solo activities (e.g., browsing on a smartphone, writing a personal journal).	Shared activities (e.g., family gaming, group exercise, conversations captured by smart speakers).	T1, T2
Device	Personal devices (e.g., smartphone, smartwatch) – Device is used only by the owner.	Shared devices (e.g., smart speakers, security cameras, shared tablet) – Any data captured, even if only one person is using it, is still collective.	T2, T4
Involvement	Direct – The person intentionally interacts with the device and generates data.	Indirect – Data is generated through ambient collection (e.g., voice assistants picking up conversations, cameras recording presence) or one can access/view the data.	T3, 4
Relationship	Data remains within the individual's control.	Data is accessible to family members, regular visitors (e.g., housekeeper), or even bystanders.	T3, T5

4.1.1 Conceptual Articulation of OurData. Across families, participants offered diverse interpretations of what counts as OurData. These interpretations were shaped by social, spatial, temporal, and technical dimensions (Table 2). Importantly, the dimensions appeared across multiple themes rather than aligning one-to-one, serving as interpretive lenses rather than mutually exclusive categories. From our analysis, five main themes emerged (T1–T5), each reflecting a distinct reasoning pattern that families applied to define or contest group data boundaries. These themes were articulated both abstractly and through reflections on the three shared sensing scenarios, clarifying how families interpret OurData in both social and practical contexts.

- **T1. Shared activities in time and space**
  Participants often defined OurData as data generated through joint activities with co-presence. This reasoning was articulated most clearly in scenarios where family members engaged in activities together. For instance, in the health monitoring scenario, P1-G reflected on location and activity tracking during shared walks, saying, "*Dad and I play Pikmin together as we walk. We share our location data. I assume this is a type of family data?*" Similarly, P4-B emphasized that collectivity stems from doing things together rather than simply being co-located, noting, "*Only the data from what we do together matters.*" When this activity-based reasoning was applied across other vignettes, however, participants differed in how

narrowly they interpreted what counts as "*doing things together.*" In Vignette 3 (Home Monitoring & Safety), P3's son argued that group data only emerges through synchronized and intentional participation, stating, *"If we're just all caught on camera doing our own things, that doesn't feel like family data."* When this activity-based reasoning was applied across other vignettes, however, participants differed in how narrowly they interpreted what counts as doing things together." These contrasts show that shared activity served as an initial anchor for defining OurData, but its boundaries were continually negotiated across vignettes based on intention, coordination and everyday family practices.

- **T2. Social intimacy level**
  OurData was often framed around social intimacy and relational closeness, with participants emphasizing that collective data requires mutual awareness and shared legitimacy among members. This perspective surfaced consistently across vignettes involving shared devices and monitoring technologies. P4-F described family data as requiring mutual awareness and agreement among members, stating, *"I think group data is only applicable to socially intimate groups. It's like a membership. You are aware that you're in it, and you can fully exercise your rights equally with others who are in it."* Similarly, P7-F drew a clear boundary around family membership, emphasizing, *"Beyond family, things get too complicated."*
  This emphasis on social intimacy shaped how participants reasoned about people who were present in the data but ambiguously positioned within the social group. In Vignette 2 (Device Sharing), while nannies or frequent helpers were often informed that their voices might be recorded, they were not always considered part of OurData. P6-M explained, *"We tell the nanny that the speaker records voices, and she can use it for commands, but that doesn't mean the data is family data in the same way."* By contrast, incidental users such as guests or delivery workers were more clearly excluded. P8-F noted, *"Bystanders didn't agree to be part of the system. They shouldn't be included just because their voices were captured."* P1-F remarked, *"Guests have rights over their data, but they're not contributors to our family data."* These examples illustrate that collective data boundaries were shaped less by data presence and more by social recognition and perceived legitimacy within the group.
- **T3. Individual attribution and contribution**
  Disagreements about whether data should be considered OurData often hinged on perceptions of who meaningfully contributed to the data and to whom it could be attributed. Across vignettes, participants evaluated not simply co-presence, but whose actions were seen as constituting the data within family practices. In Vignette 3 (Home Monitoring & Safety), participants emphasized identifiable individual behavior as a reason to resist collective framing. P9-G explained, *"If I'm the only one dancing in front of the smart camera while other family members are just passing by, it feels like I'm the only one contributing to the data."*
  At the same time, participants described how individually attributable data could still be treated as OurData when embedded in shared family routines. In Vignette 1 (Family Health Management & Monitoring), health and activity data were seen as originating from individuals but becoming collective through joint review and use. P8-M noted, *"We look at the data together as a family, but each record still comes from a specific person."* Together, these perspectives show that individual attribution did not function as a fixed boundary, but as a negotiated factor in determining when and how data could be treated as OurData within the household.
- **T4. Use purpose and context**
  Families interpreted data ownership primarily through the *purpose* and *context* of device use, rather than assuming that shared devices or co-presence automatically produced OurData. Across vignettes, participants focused on why a device was used and for whom, using these considerations to distinguish personal from collective data. This reasoning was most explicit in Vignette 2 (Device Sharing). When the smart speaker was used for individual purposes, such as searching for information or playing music alone, the resulting

data was often framed as personal despite the device being shared (P8-G2: *"If the purpose was personal, then it's personal data."*). By contrast, when the same device supported explicitly family-oriented activities, such as joint games or commands, participants described the data as collective (P4-F).
Similar distinctions appeared across other vignettes. Participants differentiated between data generated for shared family goals (e.g., monitoring children or managing family health) and data reflecting isolated individual activities. Even when data was produced in shared spaces or later discussed collectively, solo-oriented use was often treated as personal, whereas data tied to shared intentions or responsibilities was more readily treated as OurData. Overall, spatial co-location or shared access informed participants' reasoning but did not determine it on their own; instead, purpose and intended use functioned as key lenses through which families negotiated whether data should be treated as personal or collective.

- **T5. Technical definitions and data accessibility**
Some families defined OurData primarily through *technical structures and access rights* rather than shared activity or social meaning. Across vignettes, participants emphasized how data were aggregated and made accessible within the household, treating system design as a key determinant of collectivity. In Vignette 1 (Family Health Management & Monitoring), family health data was often described as a technical grouping of individual records rather than data produced together. As P2-F noted, *"Family health data feels like the sum of each person's data. It's grouped by the system, not because we created it together."*
Accessibility further shaped interpretations in Vignettes 2 and 3. Some participants argued that data became collective when it was visible or manageable by all family members, regardless of who generated it. As P4-M explained, *"If everyone in the family can access it, then it becomes family data."* In this framing, OurData was constituted less by shared experience and more by how systems configured aggregation and access.

4.1.2 Typology of OurData. Based on families' interpretations and negotiations across the vignettes, we propose a typology that clarifies how different forms of data come to be understood as OurData within households (see Table

Table 3. Typology of OurData.

Term	Scope / Example	Attribute	How it becomes OurData
Proactive Interpersonal Data	Data actively generated through joint participation or social interaction.	Active co-participation and mutual awareness.	Because people actively engage together in creating the data, ownership is seen as naturally collective.
Ambient Co-produced Data	Data generated through multiple individuals' intentional or incidental contributions, often captured by pervasive sensing technologies in a shared environment.	Incidental or ambient contribution without full awareness.	Since the environment captures everyone's contributions—whether intentional or not—the data comes to represent the group collectively.
Shared Personal Data	Data initially created by an individual but made accessible to others, either through intentional sharing or system-mediated exposure.	System-driven or intentional exposure to others.	Even if the data was generated individually, when others can access or are affected by it, it transforms into shared data and is collectively interpreted.
OurData	Includes all of the above categories.	Social context + technological mediation. Data is constituted through relationships, environments, devices, activities, and other factors not solely attributable to any one individual.	Data emerges from shared contexts and mediated environments, where ownership is no longer solely individual.

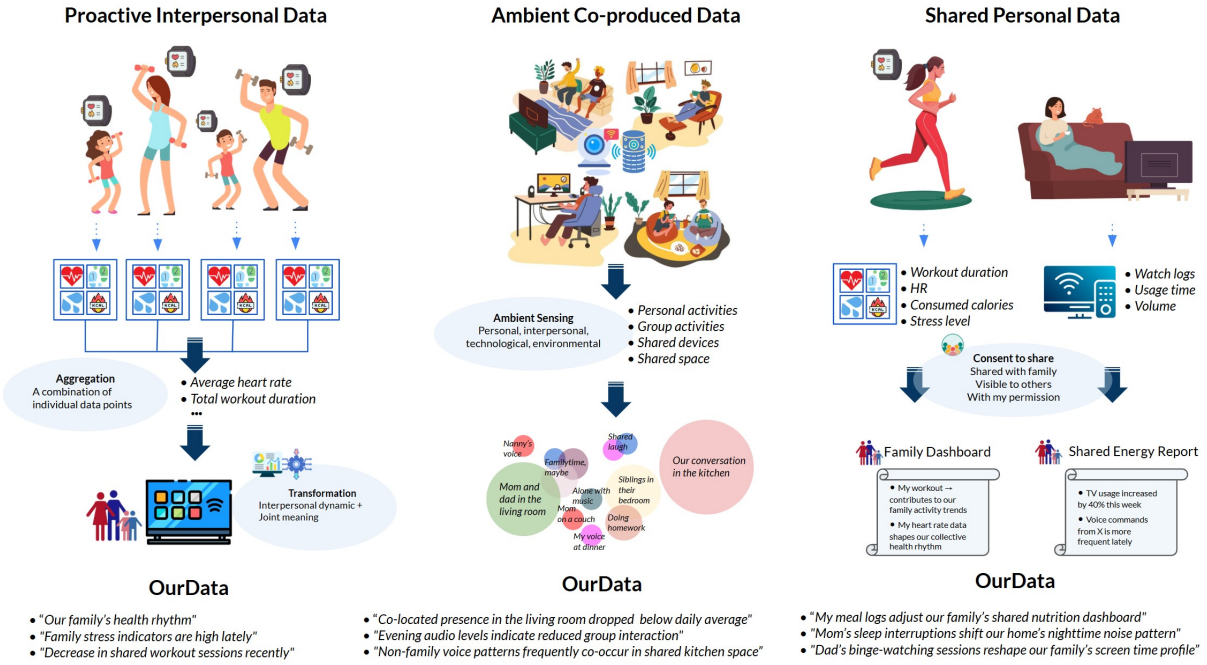

Fig. 6. Illustrative cases of OurData: Each type reflects different mechanisms of data generation and interpretation, clarifying how individually or jointly produced data can become socially perceived and collectively owned.

3, Figure 6). Rather than categorizing data solely by technical characteristics, this typology reflects how family members reasoned about shared data in everyday domestic contexts, drawing on activity, co-presence, attribution, purpose, and access. To develop this typology, we conducted thematic coding of interview data, focusing on recurring patterns in how participants described the generation, visibility, and use of data in shared family environments. The resulting categories capture not only how data is produced through sensing technologies, but also how families socially constructed data as collective through joint activities, shared routines, and negotiated boundaries. In doing so, the typology formalizes the concept of OurData as it emerged from families' lived experiences rather than from predefined system assumptions.

- **Proactive Interpersonal Data** refers to data that is intentionally created through joint participation among family members who are engaged in a shared activity. Unlike prior conceptualizations of interpersonal data, which often emphasize data that incidentally reveals information about others through sensing or inference, proactive interpersonal data emerges from situations where family members knowingly engage in a collective activity with the understanding that data will be generated and shared at the family level. In these cases, family members explicitly recognized their mutual involvement and understood the resulting data as belonging to the family unit. Examples include families playing multiplayer games together on a shared smart display or jointly exercising while tracking activity through connected devices. Such data closely aligns with participants' emphasis on shared activity and co-presence (T1), where collectivity stemmed from "doing things together" as a family.
- **Ambient Co-produced Data** refers to data that emerges from the overlapping presence and actions of multiple family members in shared domestic spaces, often captured passively by sensing technologies. Family

conversations partially recorded by smart speakers, or motion and sound data generated as household members move through common areas, were frequently discussed as examples of data that no single individual fully authored. While contributions were sometimes incidental, families often treated this data as collective because it reflected everyday family life and routines, echoing participants' reasoning around social intimacy and shared environments (T2, T4).

- **Shared Personal Data** refers to data that originates from an individual family member but becomes socially collective through visibility, access, or use within the household. Health, activity, or behavioral data generated by personal devices were often discussed in this way. Although such data remained tied to individual bodies or actions, families described how reviewing, managing, or acting on this data together shifted its meaning and governance into a shared domain. This category reflects participants' negotiations around individual attribution and access (T3, T5), where data was not fully detached from the individual but nonetheless treated as part of family-level decision making.

Overall, these findings show that families did not treat OurData as a fixed category determined solely by device type or data modality, even though both clearly shaped how data was initially perceived. Instead, families constructed OurData through ongoing social reasoning that integrated device characteristics with shared activities, family relationships, individual contribution, use purpose, and access. Across vignettes, participants moved fluidly between abstract notions of "family data" and situated judgments grounded in everyday domestic practices, often revising their interpretations as they considered specific devices and scenarios. This process reveals OurData as a negotiated and context-dependent construct, shaped by both the technical properties of sensing technologies and families' social interpretations of how those technologies fit into household life. By articulating these interpretive patterns and the resulting typology, RQ1 clarifies how collective data becomes meaningful in families, providing a foundation for examining how such meanings translate into privacy expectations, governance, and negotiation practices in shared sensing environments.

4.2 Privacy Concerns and Expectations in Managing OurData

This section answers RQ2: *"What kinds of privacy concerns and expectations emerge in these shared sensing contexts, and how are they shaped by family relationships, roles, and everyday practices?"*

4.2.1 Shaping OurData: Sensitivity and Social Context. We examined how families interpreted the sensitivity of different data types and whether related privacy risks were understood as personal or collective.

- **Physiological Data: Personal data but harmless** Participants treated physiological data (e.g., heart rate, sleep patterns) as primarily personal and low-risk despite its identifiability. As P3-F noted, *"They're just figures—what can you do with my heart rate?"* However, when such data were collected in shared spaces, some participants acknowledged that they could raise questions of shared responsibility within the household.
- **Health Data: Reframed as sensitive and collective** In contrast, when physiological data was translated into health-related information at the service layer (e.g., diagnoses, mental health, menstrual cycles), perceptions significantly shifted. Health data were widely regarded as sensitive and collectively relevant, particularly in families managing ongoing conditions, where shared responsibility reframed such data as part of OurData.
- **Audio and Video: Highly sensitive and collective** Families highlighted that these data types originate from shared devices in common spaces, making them inherently collective. Particular concern centered on children's data, as participants noted that children are less aware of privacy risks and more easily identifiable, amplifying ethical concerns and the need for careful collective governance of such data.

4.2.2 Family-Level Privacy Risks: Inference, Surveillance & Asymmetric Control. Participants often framed privacy threats as collective, affecting the family as a whole. We summarize the primary family-level privacy concerns below.

1. Inference.

- **Health Status Inference:** Families with chronic conditions or health histories were sensitive to stigmatization and unwanted exposure. P2-M said, *"Even anonymized data about my son combined with other family data could identify him."* P1-F worried about aggregated family data being compared to other families, feeling it could misrepresent them. Mothers also raised concerns about children's health data, such as menstrual tracking, emphasizing that breaches could compromise the family's collective privacy.
- **Lifestyle Profiling:** Participants noted that passive sensing (appliance use, sleep, IoT devices) could expose family routines and patterns. P6-F said, *"All these connected devices might overexpose and profile our family routines."* P2-M highlighted that combined logs reveal daily rhythms, not just individual behavior.
- **Ideological and Social Profiling:** Families worried about classification or stereotyping based on conversations or social values captured by smart speakers. P7-M stated, *"Conversations reflect intentions and values. That's why I see it as family data, not just mine or others'."*
- **Family Dynamics:** Concerns extended to sensitive family interactions such as conflicts or emotions being recorded unintentionally, adding another layer of collective privacy risk.

2. Surveillance & Asymmetric Control.

- **External Surveillance:** Families feared hacking, unauthorized storage, or misuse of audio/video data, particularly of children. P4-F described this as *living with a one-way mirror*, reflecting anxiety about data persistence and third-party access.
- **Internal Surveillance:** Cameras and smart home systems could reproduce power asymmetries. P5-M noted, *"It's like only one person gets to watch everyone else."* Default admin roles often reinforced hierarchical control, creating internal privacy tensions.
- **Asymmetric Control:** Children were concerned about parental access to data from private areas (bedrooms), emphasizing control over visibility and consent. P7-B said, *"It doesn't feel right if I don't know what's recorded about me."* Parents often saw oversight as protection, though some acknowledged the need to respect children's evolving autonomy over family-level data.

4.2.3 Expectations for Managing OurData. Participants voiced concerns about how OurData should be stored, retained, and accessed. These concerns reflect two distinct privacy regimes: (1) external risks related to institutional data control, such as third-party exposure or misuse; and (2) intra-family tensions involving relational boundaries and fairness around data access within the household. We organize participant responses accordingly.

- **External Expectations**
  - **Data Retention:** Participants were uneasy about how long their data is stored by cloud services or third parties, fearing that prolonged retention could lead to unintended exposure or misuse. For example, some worried that even mundane data could later be used for profiling by insurance companies or governments.
  - **Data Storage:** There was discomfort about the lack of transparency regarding where data is stored and how securely it is managed. Cloud-based and smart home platforms were met with skepticism, especially when storage locations or protocols were opaque. P10-M noted, *"We can try to protect our data locally at home, but once it's out, like sent to a server, I don't think we have any real control anymore. I think where and how they store them is not clearly delivered to users."* Participants desired features such as configurable expiration periods and minimized long-term external storage.

  - **Data Access & Control:** Ethical concerns were raised over third-party access to family data. Participants struggled to identify who should give their consent to govern data representing multiple members of the household. There was strong opposition to third-party use of their data [48].
- **Intra-Family Expectation**
  - **Data Retention:** Families preferred shorter retention of sensitive or personal data collected within the home, especially related to private moments or children's activities. For instance, P8-G1 emphasized, *"I want the data from my room to disappear quickly. It feels weird to think my parents or someone else might still see it later."*
  - **Data Storage:** Participants wanted transparency and control over where data is stored within shared household systems. They hoped for mechanisms to restrict access based on consent from all relevant family members and to review or adjust data handling as relationships evolve.
  - **Data Access & Control:** Managing access within families was described as challenging, especially as single actions (e.g., activating a smart speaker) might inadvertently expose data about multiple people. Parents reported making decisions on behalf of children but acknowledged that this could oversimplify complex privacy dynamics involving non-initiators or guests.

5 DISCUSSION

This study examined how families interpret, negotiate, and manage shared sensing data in everyday domestic environments, leading to the articulation of *OurData* as a situated way of reasoning about collective data. Our findings highlight how families dynamically construct its meaning through social relationships, shared routines, device affordances, and ethical considerations.

5.1 OurData for Family Privacy as Contextual, Plural, and Socially Constructed

Participants described OurData not as a fixed data category, but as a contextual construct emerging through family relationships, domestic routines, and shared sensing environments. Rather than assuming data to be inherently individual or collective, families interpreted it relationally based on how it was produced, surfaced, and made meaningful in everyday life. For example, health data collected via personal trackers was often initially understood as individual, yet reinterpreted as shared when embedded in co-monitored routines such as caregiving or shared health goals. Importantly, participants did not rely on fixed rules to determine whether data constituted OurData. Instead, they described making contextual judgments based on household roles, situational relevance, and patterns of circulation. To capture this reasoning, we draw on the notion of *semi-common*, which captures situations in which data remains individually produced, yet is treated as shared in practice (e.g., food assumed to be shared in a family refrigerator) [24, 27]. This characterization highlights OurData as fluid and plural, shaped through ongoing social interpretation rather than formal ownership boundaries. OurData is best understood not as a static object, but as an ongoing process of social meaning-making shaped by visibility and relational dependency. This perspective aligns with third-wave HCI and embodied interaction approaches [20, 21, 36], which emphasize that data and privacy emerge from socially and contextually situated practices rather than fixed technical definitions.

5.2 Rethinking Privacy Risks as Collective Exposure in Smart Homes

Consistent with prior smart home research, participants described privacy risks such as surveillance, inference, and loss of control [13, 73, 83]. However, these risks were rarely framed as purely individual harms. Instead, participants emphasized *collective exposure*, where data about one family member implicated others or the household as a whole. This perspective aligns with theoretical work on group and collective privacy, which emphasizes that group data cannot be reduced to individual consent or control [49, 70].

Such concerns can be explained through multiple forms of *privacy dependency* [7]. First, *tie-based dependencies* were salient in shared domestic routines. Data generated by one person, such as voice commands, health metrics, or presence data, was perceived as revealing information about others who shared the same space or practices, implicating family members who were not the intended subjects of data collection. Second, participants described *similarity-based dependencies*, where aggregated household data enabled profiling of the family as a whole. Patterns derived from shared routines, health data, or everyday voice interactions were seen as categorizing the household over time, echoing prior concerns about inference and secondary use in sensing systems [13, 42]. Finally, *difference-based dependencies* emerged when deviations from household norms heightened exposure. Data related to children, elderly parents, or family members with health conditions became more identifiable precisely because they did not conform to aggregated patterns, resulting in disproportionate exposure within collective data traces. These dynamics were further shaped by internal power asymmetries. Echoing prior work on parental monitoring [38, 83], participants described tensions between care, safety, and autonomy when sensing technologies blurred voluntary disclosure and passive capture in shared spaces.

5.3 Managing OurData Through Collective and Ethical Awareness

Participants approached the management of OurData not as a matter of technical control, but as ethical judgment embedded in family relationships. Rather than focusing on formal consent or ownership, they reasoned about who might be affected by data practices and who should bear responsibility for their consequences. Participants emphasized awareness and fairness, evaluating data practices based on whether others were sufficiently informed, whether data capture felt appropriate in context, and whether the burdens of sensing were unevenly distributed. Ambient data collection in shared spaces raised concerns not because it violated explicit rules, but because it implicated people who were unaware, unable to object, or disproportionately exposed, such as children or visitors. This orientation reflects a shift from individual rights toward relational responsibility. Participants framed shared data as carrying obligations toward others, managing privacy as a shared ethical concern shaped by care, accountability, and everyday family judgment rather than individual consent or technical control. This aligns with values-and-ethics perspectives in HCI [66] and highlights the limits of notice-and-consent models in sensor-rich family environments.

5.4 A Relational and Family-Centered Perspective on Group Privacy

Bringing together the findings in Sections 5.1–5.3, OurData clarifies how privacy is experienced and reasoned about in sensor-rich homes. It is not a new type of data, nor does it replace existing group or collective privacy concepts. Prior work on family and group privacy emphasizes governance, rights, coordination, shared exposure, and asymmetric control. While these remain important, our study shows that in family smart sensing, privacy reasoning often begins earlier: participants first encounter data as inherently "*about us*," shaped by shared routines, roles, and responsibilities, highlighting a moment of *relational sensemaking* that has been less explicitly theorized. We term this orientation OurData. Rather than replacing existing concepts, it complements the literature by foregrounding a phenomenological and relational stance toward sensing data, particularly salient in family smart home environments where data is ambient, inferred, and temporally extended. By making this layer of everyday sensemaking explicit, OurData helps articulate dimensions of family and group privacy that remain difficult to capture using existing terms alone, providing a lens to understand how privacy emerges as a lived, relational process before questions of ownership, control, or formal governance arise.

5.5 Design Implications

5.5.1 Supporting Consent for Group Privacy. Participants understood OurData as emerging from shared contexts, not merely aggregated personal data. This highlights a gap in conventional consent models, which often assume individual decision-making and overlook collective dynamics. In sensor-rich environments, these dynamics are amplified as ambient devices continuously capture data across spaces and users, making it difficult to manage privacy without accounting for relational and contextual factors.

Our findings suggest consent mechanisms in ubiquitous sensing environments should support negotiation among multiple stakeholders [86], allow real-time social control in public or semi-public settings [12], and balance individual privacy with collective benefit through group-level utility frameworks [39, 69]. Consent should be continuous, context-aware, and sensitive to social roles and norms, enabling the system to adapt as relationships and spaces evolve [26, 44, 46].

We also emphasize the inclusion of passive or unaware participants, for instance via delegated consent models where trusted entities (e.g., socially attuned AI agents) that act on behalf of others [23, 31, 58]. Building on the OurData concept, we envision an "*OurAgent*" that mediates group preferences, signals silent stakeholders, and supports coordinated, fair consent in multi-user sensing environments. By explicitly designing for relational accountability and ethically informed adaptation, this approach operationalizes group privacy principles in ubiquitous sensing environments, offering concrete guidance for designers of homes, workplaces, and other multi-user contexts where data is continuously captured and shared.

Beyond improving notice and consent mechanisms, our findings point to broader design opportunities for rethinking how privacy is operationalized in multi-user sensing environments. In this sense, our work aligns with prior critiques of individual-centric consent models [28, 68], and suggests future research directions that explore alternative paradigms for supporting collective sensemaking, accountability, and agency around shared data.

5.5.2 Visualizing Social Context in Ubiquitous Sensing. Participants often struggled to recognize when individually collected data also implicated others. In ubiquitous sensing environments, even actions like activating a smart speaker could produce data about the entire household. This highlights the need for systems that make the *social scope* of OurData legible, indicating what is collected, who is affected, and in which contexts. Interfaces can use visual cues, prompts, or collective metaphors (e.g., multi-user timelines, shared dashboards) to represent data as a group-level artifact [41, 79, 80].

Feedback that reveals ripple effects, such as *"This sleep log may reveal your partner's routine"*, helps users reflect ethically and recognize implications for non-initiators like housemates or visitors. Designs should consider layers of social visibility: *cohabitants* (family), *intimate others* (friends), and *bystanders* (strangers) [51]. Tangible or multimodal cues (LEDs, auditory alerts, visual prompts) support *awareness by design* [2, 43, 52], allowing users to navigate blurred boundaries between individual and collective data.

Features such as real-time bystander detection, post-capture visibility, and tools to obscure non-primary users [37, 53] further enable situated, collective decisions. By visualizing social context and providing interactive cues, these designs leverage ubiquitous sensing to support relational accountability, informed consent, and collective privacy management in shared environments.

5.5.3 Empowering Situated and Collective Control of OurData. Participants understood ubiquitous sensing environments as socially situated systems that reshape relationships and accountability. Spaces like kitchens and living rooms, and devices such as smart speakers, were experienced as collective technologies grounded in social roles and ongoing interactions. However, current infrastructures treat sensing as individually owned and static, often producing one sided visibility or surveillance that conflicts with users' expectations

for shared environments. This mismatch reveals how design choices constrain opportunities for collective reflection, mutual respect, and ethical management of shared data.

To align ubiquitous sensing with social context, systems should detect and respond to multi-user dynamics and situational boundaries [86]. Devices can adjust data collection based on who is present, their roles, and the nature of the interaction [22, 62]. For example, they may reduce detail during group conversations or label areas as collective zones that require broader consent and awareness. Building on the principles of *social translucence* [25], socially responsive sensing makes participants' presence, activities, and data visibility legible to one another, supporting awareness and accountability across cohabitants. Interfaces should also enable collaborative reinterpretation and management of data. Controls like *"switch to shared," "blur others,"* or *"flag as group data"* support both real-time and retrospective negotiation of visibility, offering shared governance rather than individual gatekeeping [55, 57]. Drawing from research on preference elicitation, systems can help cohabitants establish sensing boundaries together, reducing power asymmetries and supporting fair participation in household data practices.

Designing for OurData means treating sensing as a process of ongoing social negotiation, where social translucence ensures that collective presence and activities are visible, interpretable, and negotiable. This contributes to ubiquitous computing by articulating principles for adaptive and ethically aware systems that recognize the collective nature of data and empower people to manage it through situated and shared control.

6 LIMITATIONS

While our study provides insights into how families interpret interpersonal data in sensor-rich homes, it has several limitations. Our sample (N = 34) consisted of families familiar with sensing technologies within a single national context, which may not reflect the perspectives of more tech-averse or marginalized groups. In addition, our participants were primarily dual-parent households with children in a relatively narrow age range, which may limit how broadly our findings capture variations in family structures and life stages. The ways in which OurData is constructed and negotiated may differ in other contexts, such as single-parent families, multi-generational households, or families with older or younger children. Our focus on family households also excludes other living arrangements and non-domestic smart environments (e.g., shared housing, workplaces, or semi-public spaces) or other relational configurations (e.g., child-owned devices), where privacy dynamics may differ. In addition, the use of family co-interviews may have limited the disclosure of sensitive intra-family disagreements, despite efforts to mitigate power imbalances. Finally, while speculative vignettes supported reflection on potential risks, they cannot fully capture real-world complexities, and scenario design may have influenced participants' perceptions. Future work should therefore examine collective data practices through longitudinal and cross-context studies.

7 CONCLUSION

As sensing technologies become embedded in everyday environments, data must be understood relationally, shaped by shared practices, roles, and contexts. Our study reframes sensing not as neutral infrastructure but as a site of social negotiation. The concept of OurData highlights how users navigate data as coinhabitants, balancing boundaries and responsibilities. This perspective calls for design frameworks that foster collective awareness, contextual consent, and interpersonal boundary management. Future sensing systems should act as socially responsive participants, adapting to multi-user dynamics and supporting ethical, inclusive ways of living, sharing, and caring together.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(RS-2023-00273957) and supported by the 2026 G-School International Joint Research Program at the Korea Advanced Institute of Science and Technology (KAIST), funded by the Ministry of Science and ICT of the Republic of Korea (N10260081).

References

[1] Shane Ahern, Dean Eckles, Nathaniel S Good, Simon King, Mor Naaman, and Rahul Nair. 2007. Over-exposed? Privacy patterns and considerations in online and mobile photo sharing. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. 357–366.

[2] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J Lee. 2020. Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), 1–28.

[3] Ifeoma Ajunwa. 2018. Algorithms at work: productivity monitoring applications and wearable technology as the new data-centric research agenda for employment and labor law. . *Louis ULJ* 63 (2018), 21.

[4] Bayan Al Muhander, Jason Wiese, Omer Rana, and Charith Perera. 2023. Interactive privacy management: Toward enhancing privacy awareness and control in the Internet of Things. *ACM Transactions on Internet of Things* 4, 3 (2023), 1–34.

[5] Irwin Altman. 1975. The environment and social behavior: privacy, personal space, territory, and crowding. (1975).

[6] Noah Apthorpe, Dillon Reisman, and Nick Feamster. 2017. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *arXiv preprint arXiv:1705.06805* (2017).

[7] Solon Barocas and Karen Levy. 2020. Privacy dependencies. *Wash. L. Rev.* 95 (2020), 555.

[8] Andrew Besmer and Heather Richter Lipford. 2010. Moving beyond untagging: photo privacy in a tagged world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 1563–1572.

[9] Gergely Biczók and Pern Hui Chia. 2013. Interdependent privacy: Let me share your data. In *Financial Cryptography and Data Security: 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers 17*. Springer, 338–353.

[10] Danah Boyd. 2012. Networked privacy. *Surveillance & society* 10, 3/4 (2012), 348.

[11] Virginia Braun and Victoria Clarke. 2021. One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative research in psychology* 18, 3 (2021), 328–352.

[12] Youngjae Chang, Sookyung Han, Hyunjong Lee, Seungchul Lee, Wonjung Kim, Jinu Choi, Chloe Ann McCracken, and Junehwa Song. 2024. Understanding Instant Social Control of Shared Devices in Public Spaces: A Field Trial. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 8, 3 (2024), 1–33.

[13] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, and Julie A Kientz. 2011. Living in a glass house: a survey of private moments in the home. In *Proceedings of the 13th international conference on Ubiquitous computing*. 41–44.

[14] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N Patel, and Julie A Kientz. 2012. Investigating receptiveness to sensing and inference in the home using sensor proxies. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*. 61–70.

[15] Andy Crabtree, Hamed Haddadi, and Richard Mortier. 2022. Privacy by Design for the Internet of Things. *Privacy by Design for the Internet of Things: Building Accountability and Security (2021)* (2022). https://shop.theiet.org/privacy-by-design-for-the-internet-of-things

[16] Andy Crabtree and Richard Mortier. 2015. Human data interaction: historical lessons from social studies and CSCW. In *ECSCW 2015: Proceedings of the 14th European Conference on Computer Supported Cooperative Work, 19-23 September 2015, Oslo, Norway*. Springer, 3–21.

[17] Andy Crabtree and Richard Mortier. 2016. Personal data, privacy and the internet of things: the shifting locus of agency and control. *Privacy and the Internet of Things: The Shifting Locus of Agency and Control (November 22, 2016)* (2016).

[18] Audrey Desjardins and Heidi R Biggs. 2021. Data epics: Embarking on literary journeys of home internet of things data. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–17.

[19] Audrey Desjardins, Heidi R Biggs, Cayla Key, and Jeremy E Viny. 2020. IoT data in the home: Observing entanglements and drawing new encounters. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–13.

[20] Paul Dourish. 2001. *Where the action is: the foundations of embodied interaction*. MIT press.

[21] Paul Dourish and Ken Anderson. 2006. Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-computer interaction* 21, 3 (2006), 319–342.

[22] Micha Drozdowicz, Maria Ganzha, and Marcin Paprzycki. 2020. Semantic access control for privacy management of personal sensing in smart cities. *IEEE Transactions on Emerging Topics in Computing* 10, 1 (2020), 199–210.

[23] Rachel Eardley, Sue Mackinnon, Emma L Tonkin, Ewan Soubutts, Amid Ayobi, Jess Linington, Gregory JL Tourte, Zoe Banks Gross, David J Bailey, Russell Knights, et al. 2022. A case study investigating a user-centred and expert informed'companion guide'for a complex sensor-based platform. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 6, 2 (2022), 1–23.

[24] Robert C Ellickson. 2006. Unpacking the household: informal property rights around the hearth. *Yale LJ* 116 (2006), 226.

[25] Thomas Erickson and Wendy A Kellogg. 2000. Social translucence: an approach to designing systems that support social processes. *ACM transactions on computer-human interaction (TOCHI)* 7, 1 (2000), 59–83.

[26] Lujun Fang and Kristen LeFevre. 2010. Privacy wizards for social networking sites. In *Proceedings of the 19th international conference on World wide web*. 351–360.

[27] Lee Anne Fennell. 2011. Ostrom's Law: Property rights in the commons. *International Journal of the Commons* 5, 1 (2011).

[28] Anne Josephine Flanagan, Jen King, and Sheila Warren. 2020. Redesigning data privacy: Reimagining notice & consent for human-technology interaction. In *World Economic Forum*.

[29] Martin Flintham, Murray Goulden, DOMINIC PRICE, and Lachlan Urquhart. 2018. 20: DOMESTICATING DATA: SOCIO-LEGAL PERSPECTIVES ON SMART HOMES AND GOOD DATA DESIGN. *Good Data* 20 (2018), 343.

[30] Christine Geeng and Franziska Roesner. 2019. Who's in control? Interactions in multi-user smart homes. In *Proceedings of the 2019 CHI conference on human factors in computing systems*. 1–13.

[31] Ilche Georgievski, Isaac Henderson Johnson Jeyakumar, and Shrilesh Kale. 2021. Designing a system based on robotic assistance for privacy awareness in smart environments. In *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. IEEE, 0427–0432.

[32] Murray Goulden, Peter Tolmie, Richard Mortier, Tom Lodge, Anna-Kaisa Pietilainen, and Renata Teixeira. 2018. Living with interpersonal data: Observability and accountability in the age of pervasive ICT. *New Media & Society* 20, 4 (2018), 1580–1599.

[33] Jonathan Grudin. 2002. Group dynamics and ubiquitous computing. *Commun. ACM* 45, 12 (2002), 74–78.

[34] Neilly H. Tan, Richmond Y. Wong, Audrey Desjardins, Sean A. Munson, and James Pierce. 2022. Monitoring pets, deterring intruders, and casually spying on neighbors: Everyday uses of smart home cameras. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–25.

[35] Steve Harrison and Paul Dourish. 1996. Re-place-ing space: the roles of place and space in collaborative systems. In *Proceedings of the 1996 ACM conference on Computer supported cooperative work*. 67–76.

[36] Steve Harrison, Deborah Tatar, and Phoebe Sengers. 2007. The three paradigms of HCI. In *Alt. Chi. Session at the SIGCHI Conference on human factors in computing systems San Jose, California, USA*. 1–18.

[37] Rakibul Hasan, David Crandall, Mario Fritz, and Apu Kapadia. 2020. Automatically detecting bystanders in photos to reduce privacy risks. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 318–335.

[38] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. 2018. Rethinking access control and authentication for the home internet of things ({{{{{IoT}}}}}). In *27th USENIX Security Symposium (USENIX Security 18)*. 255–272.

[39] Mathias Humbert, Benjamin Trubert, and Kévin Huguenin. 2019. A survey on interdependent privacy. *ACM Computing Surveys (CSUR)* 52, 6 (2019), 1–40.

[40] William Jang, Adil Chhabra, and Aarathi Prasad. 2017. Enabling multi-user controls in smart home devices. In *Proceedings of the 2017 workshop on internet of things security and privacy*. 49–54.

[41] Yanqi Jiang, Xianghua Ding, Xiaojuan Ma, Zhida Sun, and Ning Gu. 2023. IntimaSea: exploring shared stress display in close relationships. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–19.

[42] Predrag Klasnja, Sunny Consolvo, Jaeyeon Jung, Benjamin M Greenstein, Louis LeGrand, Pauline Powledge, and David Wetherall. 2009. " When I am on Wi-Fi, I am fearless" privacy concerns & practices in eeryday Wi-Fi use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 1993–2002.

[43] Marc Langheinrich. 2001. Privacy by design—principles of privacy-aware ubiquitous systems. In *International conference on ubiquitous computing*. Springer, 273–291.

[44] Hyunsoo Lee, Yugyeong Jung, Hei Yiu Law, Seolyeong Bae, and Uichin Lee. 2024. PriviAware: Exploring Data Visualization and Dynamic Privacy Control Support for Data Collection in Mobile Sensing Research. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–17.

[45] Hyunsoo Lee, Yugyeong Jung, Youwon Shin, Hyesoo Park, Woohyeok Choi, and Uichin Lee. 2024. FamilyScope: Visualizing Affective Aspects of Family Social Interactions using Passive Sensor Data. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW1 (2024), 1–27.

[46] Hyunsoo Lee and Uichin Lee. 2022. Toward dynamic consent for privacy-aware pervasive health and well-being: A scoping review and research directions. *IEEE pervasive computing* 21, 4 (2022), 25–32.

[47] Anna Lenhart, Sunyup Park, Michael Zimmer, and Jessica Vitak. 2023. " You Shouldn't Need to Share Your Data": Perceived Privacy Risks and Mitigation Strategies Among Privacy-Conscious Smart Home Power Users. *Proceedings of the ACM on*

Human-Computer Interaction 7, CSCW2 (2023), 1–34.
[48] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019).
[49] Alessandro Mantelero. 2017. From group privacy to collective privacy: towards a new dimension of privacy and data protection in the big data era. *Group privacy: new challenges of data technologies* (2017), 139–158.
[50] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. 2020. Smart devices in Airbnbs: Considering privacy and security for both guests and hosts. *Proceedings on Privacy Enhancing Technologies* (2020).
[51] Panos Markopoulos and Wendy Mackay. 2009. *Awareness systems: Advances in theory, methodology and design.* Springer Science & Business Media.
[52] Karola Marky, Nina Gerber, Michelle Gabriela Pelzer, Mohamed Khamis, and Max Mühlhäuser. 2022. "You offer privacy like you offer tea": Investigating mechanisms for improving guest privacy in IoT-equipped households. *Proceedings on Privacy Enhancing Technologies* (2022).
[53] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. 2020. " I don't know how to protect myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*. 1–11.
[54] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. 2017. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI conference on human factors in computing systems*. 2189–2201.
[55] David W McDonald, Stephanie Gokhman, and Mark Zachry. 2012. Building for social translucence: a domain analysis and prototype system. In *Proceedings of the ACM 2012 conference on computer supported cooperative work*. 637–646.
[56] Nicole Meng, Dilara Keküllüoğlu, and Kami Vaniea. 2021. Owning and sharing: Privacy perceptions of smart speaker users. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–29.
[57] Karin Niemantsverdriet, Mendel Broekhuijsen, Harm van Essen, and Berry Eggen. 2016. Designing for multi-user interaction in the home environment: implementing social translucence. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*. 1303–1314.
[58] Bettina Nissen, Victoria Neumann, Mateusz Mikusz, Rory Gianni, Sarah Clinch, Chris Speed, and Nigel Davies. 2019. Should i agree? delegating consent decisions beyond the individual. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.
[59] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.
[60] Sunyup Park, Weijia He, Elmira Deldari, Pardis Emami-Naeini, Danny Yuxing Huang, Jessica Vitak, Yaxing Yao, and Michael Zimmer. 2024. Well-intended but half-hearted:{Hosts'} consideration of {guests'} privacy using smart devices on rental properties. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. 179–198.
[61] Sandra Petronio. 2017. Communication privacy management theory: Understanding families. In *Engaging theories in family communication*. Routledge, 87–97.
[62] Blaine A Price, Karim Adam, and Bashar Nuseibeh. 2005. Keeping ubiquitous computing to yourself: A practical model for user control of privacy. *International Journal of Human-Computer Studies* 63, 1-2 (2005), 228–253.
[63] Beate Roessler and Dorota Mokrosinska. 2013. Privacy and social interaction. *Philosophy & Social Criticism* 39, 8 (2013), 771–791.
[64] Herman Saksono, Ashwini Ranade, Geeta Kamarthi, Carmen Castaneda-Sceppa, Jessica A Hoffman, Cathy Wirth, and Andrea G Parker. 2015. Spaceship Launch: Designing a collaborative exergame for families. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*. 1776–1787.
[65] John Shaeffer and Charlie Nelson Keever. 2021. Privacy as a collective norm. *Loy. LA Ent. L. Rev.* 41 (2021), 253.
[66] Katie Shilton et al. 2018. Values and ethics in human-computer interaction. *Foundations and Trends® in Human–Computer Interaction* 12, 2 (2018), 107–171.
[67] Stephen Snow, Awais Hameed Khan, Mashhuda Glencross, and Neil Horrocks. 2021. Neighbourhood Wattch: Using Speculative Design to Explore Values Around Curtailment and Consent in Household Energy Interactions. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–12.
[68] Daniel J Solove. 2013. Privacy self-management and the consent dilemma introduction. 1880–1903 pages.
[69] Anna Cinzia Squicciarini, Mohamed Shehab, and Federica Paci. 2009. Collective privacy management in social networks. In *Proceedings of the 18th international conference on World wide web*. 521–530.
[70] Linnet Taylor, Luciano Floridi, and Bart Van der Sloot. 2016. *Group privacy: New challenges of data technologies*. Vol. 126. Springer.
[71] Linnet Taylor, Luciano Floridi, and Bart van der Sloot. 2017. Introduction: A new perspective on privacy. *Group privacy: New challenges of data technologies* (2017), 1–12.
[72] Kurt Thomas, Chris Grier, and David M Nicol. 2010. unfriendly: Multi-party privacy risks in social networks. In *Privacy Enhancing Technologies: 10th International Symposium, PETS 2010, Berlin, Germany, July 21-23, 2010. Proceedings 10*. Springer, 236–252.

[73] Peter Tolmie, James Pycock, Tim Diggins, Allan MacLean, and Alain Karsenty. 2002. Unremarkable computing. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. 399–406.
[74] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. 129–139.
[75] Mark Weiser. 1999. The computer for the 21st century. *ACM SIGMOBILE mobile computing and communications review* 3, 3 (1999), 3–11.
[76] Richmond Y Wong, Deirdre K Mulligan, Ellen Van Wyk, James Pierce, and John Chuang. 2017. Eliciting values reflections by engaging privacy futures using design workbooks. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–26.
[77] Richmond Y Wong, Jason Caleb Valdez, Ashten Alexander, Ariel Chiang, Olivia Quesada, and James Pierce. 2023. Broadening privacy and surveillance: Eliciting interconnected values with a scenarios workbook on smart home cameras. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference*. 1093–1113.
[78] Richmond Y Wong, Ellen Van Wyk, and James Pierce. 2017. Real-fictional entanglements: Using science fiction and design fiction to interrogate sensing technologies. In *Proceedings of the 2017 Conference on Designing Interactive Systems*. 567–579.
[79] Mengru Xue, Rong-Hao Liang, Jun Hu, Bin Yu, and Loe Feijs. 2022. Understanding how group workers reflect on organizational stress with a shared, anonymous heart rate variability data visualization. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts*. 1–7.
[80] Mengru Xue, Rong-Hao Liang, Bin Yu, Mathias Funk, Jun Hu, and Loe Feijs. 2019. AffectiveWall: designing collective stress-related physiological data visualization for reflection. *IEEE Access* 7 (2019), 131289–131303.
[81] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proceedings of the 2019 chi conference on human factors in computing systems*. 1–12.
[82] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy perceptions and designs of bystanders in smart homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–24.
[83] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security and privacy concerns with smart homes. In *thirteenth symposium on usable privacy and security (SOUPS 2017)*. 65–80.
[84] Eric Zeng and Franziska Roesner. 2019. Understanding and improving security and privacy in {multi-user} smart homes: A design exploration and {in-home} user study. In *28th USENIX Security Symposium (USENIX Security 19)*. 159–176.
[85] Nan Andy Zhang, Chong Alex Wang, Yan Xu, et al. 2022. Peer privacy concern: conceptualization and measurement. *MIS Quarterly* 46, 1 (2022).
[86] Haozhe Zhou, Mayank Goel, and Yuvraj Agarwal. 2024. Bring Privacy To The Table: Interactive Negotiation for Privacy Settings of Shared Sensing Devices. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–22.

Appendix

A Interview Questions

1. General Questions (Before Scenario Walkthrough)

Perceptions of Group Data

Before the scenario walkthroughs, we asked participants general questions to understand their perceptions of group data and privacy boundaries. These questions aimed to explore how families define and differentiate personal and collective data, as well as their thoughts on privacy in shared contexts.

- How do you define *personal* versus *group* (family-level) data?
- Have you ever thought about this distinction before? Why or why not?
- Can you give examples of data you consider personal, and those you consider collective?
- Are there situations where the boundary between personal and group data becomes unclear?
- Do you think some group data still require individual-level privacy considerations?
- How do you feel about data that involves multiple people (e.g., shared spaces, shared activities)? Who should have the right to control or access such data?
- What factors or conditions make you consider data as group data rather than personal data?

2. Vignette-Based Questions

For each vignette, participants simulated interactions with the prototype. Researchers guided discussions with questions related to each component:

- **Data Types**
  - What types of sensor data are collected in this scenario?
  - Which data do you consider sensitive? Do sensitivities differ across family members?
  - Which data is considered personal in this scenario, and which can be considered as group data (family data) here?
  - Do all family members agree on which data should be treated as group data? If not, what are the differences?
- **Data Usage**
  - What are potential uses of this data? By whom and for what purposes?
  - How acceptable are these uses from your perspective?
  - Would certain uses require additional permission or agreement?
  - Should personal and group data be used differently? If so, how?
  - Who should have a say in how group data is used or shared?
  - Are there situations where using group data feels more sensitive or problematic than using personal data?
- **Data Retention**
  - For how long should each type of data be kept?
  - Should retention vary by data type or sensitivity?
  - Should there be differences in retention policies for personal data vs. group data?
  - Who should be able to access, review, or request deletion of group data?
  - How would you feel if a family member requested deletion or modification of shared (group) data?
- **Data Storage**
  - Where should this data be stored (e.g., locally vs. cloud)?
  - Should personal and group data be stored differently?
  - Who should be responsible for managing stored data?
- **Data Access and Control**
  - Who should be able to access this data?
  - Should access differ for personal vs. group data? If so, how?
  - Under what conditions should data be shared (e.g., among family members, with service providers)?
  - Should certain types of group data require mutual consent before being shared?
  - How should access permissions be negotiated, updated, or revoked over time?
  - What happens if family members disagree on who should have access to shared data?

B Vignette-Specific Responses: Situated Social Reasoning about OurData

We further examined how families' interpretations of OurData varied across three different shared sensing scenarios. We note that participants' general framings of group data and their situated responses to specific home scenarios did not always align perfectly. This divergence reflects the contextual and interpretive nature of collective data boundaries rather than any inconsistency in reasoning. Participants often started with a broad notion of sharedness, then refined or revised their stance when prompted to consider particular situations, drawing on social reasoning about relationships, roles, and practical use. Such shifts are consistent with prior findings in privacy and data use literature [5, 59, 61], which show that abstract notions of data

ownership are frequently reinterpreted in light of social context, relational dynamics, and practical concerns. In the following scenario-based findings, we annotate each item with the corresponding themes (T1–T5) to show how participants negotiated the boundaries of collective data. Their reasoning highlights not only practical considerations, but also the social norms, relationships, and values that shape how data is understood and used in everyday life.

Vignette 1: Family Health Management & Monitoring (Smartphone, Smartwatch)

- **Family as a collective data unit (T2, T5)**
  Participants viewed health data as collective when used or shared within the family. F1-F said, *"Even if it's an individual's health data, we use it together, and healthcare services often summarize it as our family, not just individuals."* Some participants argued that the health and activity data of each family member should be considered a common asset, especially when used for collective monitoring or managing family health. F2-M said: *"If we're connecting each personal health data with family health records, it's a common asset."* However, they also acknowledged that such data still originated from personal devices and retained individual significance. Some framed group data technically as a sum of personal data, suggesting its collective nature may come from computational aggregation rather than shared activities or relationships.
- **Activity-based definition (T1)**
  Participants also defined group data based on whether multiple family members engaged in *the same activity together*. Solo activities, even in shared spaces, were considered personal. F4-M explained: *"Everything except the data that was collected from the shared activities is personal data. Home is a shared space, but it's also a personal space at the same time. Even if all of us are at home, but if I'm the only one who's exercising in the living room, then that's personal."* Others (F4, F5, F6, F7, F10) showed similar responses that the collective nature of the activity itself determines whether data is shared.
- **Device and data type dependency (T3)**
  Participants stressed that the type of device producing the data determined whether it was considered personal or shared. Data generated by an individual's device remained personal, regardless of where or when it was created. F8-M described: *"I think family health data is just a sum of personal data. After all, it's all coming from an individual. You do your thing, and you may contribute. But that doesn't mean it's something we all share."* F3 and F9 similarly indicated that although data might be aggregated at a family level, its fundamental nature was still rooted in individual ownership because each piece was produced independently by personal devices.

Vignette 2: Device Sharing (Smart speaker)

- **Smart speaker as a shared device (T1)**
  Several participants likened the smart speaker to other shared household devices, highlighting its role as a medium for facilitating family activities. For example, F1 and F4 described the speaker as a tool used together for everyday tasks, similar to watching TV. F4-F said, *"We bought the speaker for family use and all of us actively use it. Regardless of personal use, I think the data from this device belongs to all."* F3, F5, and F6 similarly emphasized that the smart speaker is inherently collective because it is designed for everyone in the household, not for individual use.
- **Speaker data as a collective asset (T2)**
  Participants also described how the type of data collected by smart speakers reinforced their shared nature, shaped by the social intimacy of household interactions. F7-M highlighted the difference between speaker data and other types of personal data, stating: *"Speaker data differs from physiological data*

collected by smartphones or smartwatches because conversations reflect our thoughts and interactions. In such sense, they're group data." Similarly, F2-B1 reported: *"Family conversations recorded through the speaker are a common asset. Each voice can't be separated as personal data."*

- **Purpose and context in speaker usage (T4)**
  In the device sharing scenario, participants emphasized that the purpose behind using a device like a smart speaker determined whether the resulting data was personal or collective. When an individual used the device alone, the data was perceived as personal, even if the device itself was shared by the household. F2-M explained: *"If I use the speaker alone while others are together, that's personal data. Guests' data are also personal."* Similarly, F8-G2 stressed the importance of user purpose, stating: *"If the purpose was personal, it's personal (e.g., searching)."* These responses highlight that the mere fact that a device is shared does not automatically make all its data collective; the usage context and social interaction around the device critically shape the boundaries of OurData.
- **Boundary of contributors (T2, T5)**
  Participants showed divergent views on whether guest data should be treated as part of OurData (T2). Overall, regular visitors, such as nannies, were often considered contributors, while incidental users, like occasional guests or delivery people, were excluded. F6-M explained, *"We have a nanny coming over, and we inform her that her voice can be recorded. We registered her as a user to use commands like 'open curtain.' She has the right to be informed and is part of our family data."* F7-F emphasized that only close social intimates should count as contributors. F9-F further framed OurData through accessibility (T5), arguing that any data accessible to all family members qualifies, regardless of who created it or which device produced it. In contrast, F8-F noted that incidental users, such as bystanders, should not be part of OurData, saying: *"Bystanders didn't sign up for device use, and we don't have to inform them."* F1-F also emphasized respecting guests' rights while keeping them outside the family's collective data, stating: *"Guests should have rights over their data but are not contributors. Maybe future services can tag guest voices as not our family's data."*

Vignette 3: Home Monitoring & Safety (Smart Camera)

- **Camera data in shared spaces (T4)**
  Participants generally viewed camera data collected in shared spaces as belonging to the family as a whole. F1-F said: *"It's a 'home' camera, used together."* Similarly, F3-M emphasized: *"If the camera is in a shared space, there's no personal data. It's a family device in a group space!"* F6-M added that monitoring household members was the camera's main purpose: *"The camera is for monitoring kids and nanny. No one in our home feels uncomfortable because it's natural."*
- **Context and place determine personal vs. group data (T4, T5)**
  Some participants highlighted that camera data could shift between personal and collective depending on the context and location (T4). F1-M stated: *"Footage of me alone in the kitchen or on the sofa is personal data. It depends on space."* However, not all participants relied solely on spatial or contextual cues. Others viewed ownership based on access permissions, which played a decisive role in defining whether it was personal or shared (T5). F4-M noted *"If only I can view my footage, it's personal data; if the family can access it, it's group data."*
- **Behavioral data is personal, even in shared spaces (T3, T4)**
  Some participants argued that even in shared spaces, captured behaviors should be treated as personal data. This perspective emphasized that data ownership is grounded not just in physical context, but in the individual's identifiable actions and contributions (T3). F7-B pointed out: *"Camera footage captures individual movements and behavior, making it personal data, even if in a shared space."* Others noted

that the purpose of use, whether monitoring individual activity or family routines, shapes judgments of personal vs. collective data (T4). F5-F and F9-F emphasized individual activity over shared framing: *"Even if the family is together, different actions make it personal data. How could this be labeled as family data? Just because we're in the frame together?"*

– **Outdoor camera footage and ethical considerations (T2, T5)**
Participants also discussed footage captured outside the home, raising questions about the boundaries of shared data. Perceptions of OurData extended beyond household members, depending on the level of social intimacy (T2). F2-M and F2-F remarked: *"Outdoor cameras monitor neighbors, delivery people, and guests. They contribute to data, but there's no need to be notified."* Participants also noted that access and system settings affect ownership (T5). F4-M added, *"Bystanders outside have rights over their data but limited access. Guests inside should be considered part of the data."*