Jun 23rd, 9:00 AM - Jun 28th, 5:00 PM

Penumbra of privacy: A people-centered and place-centered approach to data privacy for smart workspaces

Isha Hans
Carnegie Mellon University, United States

Dina El-Zanfaly
Carnegie Mellon University, United States

Lorrie Faith Cranor
Carnegie Mellon University, United States

Citation

Hans, I., El-Zanfaly, D., and Faith Cranor, L. (2024) Penumbra of privacy: A people-centered and place-centered approach to data privacy for smart workspaces, in Gray, C., Ciliotta Chehade, E., Hekkert, P., Forlano, L., Ciuccarelli, P., Lloyd, P. (eds.), *DRS2024: Boston*, 23–28 June, Boston, USA. https://doi.org/10.21606/drs.2024.1004

DRS BOSTON 20 DRS 24 JUNE 24 — 28

Penumbra of privacy: A people-centered and place-centered approach to data privacy for smart workspaces

Isha Hans*, Dina El-Zanfaly, Lorrie Faith Cranor

Carnegie Mellon University, United States of America

*Corresponding e-mail: ihans@alumni.cmu.edu

doi.org/10.21606/drs.2024.1004

Abstract: Data privacy is a complex subject where current approaches primarily focus on computing-centric narratives. These approaches have proven inadequate, yet they have established the status quo for emerging technologies including IoT in workspaces, or 'smart' workspaces, disregarding the sociocultural and behavioral dimensions of privacy within spatial contexts. This paper presents two key ideas 1) advocating a theory of change that complements the computing-focused approach (the umbra), with a broader approach based on human-centered experience and values, (the penumbra); and 2) embedding this holistic privacy approach in the early stages of smart workspace innovation through a generative design process involving multidisciplinary stakeholders. The outcome of this work is the 'Designing with Privacy' toolkit for collaboration among architects, designers, IoT engineers, privacy professionals, and other relevant stakeholders. The toolkit offers 14 value-based privacy prompts for creating and refining a collectively agreed-upon privacy brief to guide the design and development of smart workspaces.

Keywords: privacy for IoT; smart buildings; value-sensitive design; multidisciplinary toolkit

1. Introduction

The existing data privacy practices have become significant and nuanced over the years. However, most of these practices evolved as a reactionary response to growing online privacy concerns. They are still in the nascent stages of asking critical questions around the ethics and qualitative aspects of data. These qualitative aspects of data, and therefore privacy approaches, are particularly underdeveloped in the context of smart building innovation. Smart buildings, often seen as hyperconnected systems of sensors, cameras, beacons, smartphones, and operating systems connected through the internet (IoT), have been reduced to a problematic metaphor - a 'computer' that can be programmed and neatly operationalized (Mattern, 2021). By extension, smart buildings, including smart workspaces, tend

to adopt privacy approaches rooted in computing-inspired narratives for online privacy. This perspective is problematic for two reasons: 1) despite the inadequacy of existing internet-based privacy models, they continue to set the status quo (or umbra) for emerging applications of technology, including IoT applications for buildings, and 2) it oversimplifies the complexity of privacy in these contexts by disregarding the sociocultural and behavioral dimensions of privacy within spatial contexts.

The insufficiency of current practices, coupled with the lack of emphasis on social and behavioral aspects of human experience, highlights the disconnect between CS (computer science) and STS (Science, Technology, and Society) perspectives. Consequently, these practices are ill-suited for their direct transference to emerging technology including IoT applications for buildings (Greenfield, 2006), where the captured data is a rich narrative of human experiences, behaviors, values, and ways of being (Friedman, 1997). For example, in the context of a workspace, most people avoid sharing too many details about their personal lives and prefer taking private calls either in a secluded area where they won't be overheard or in more public areas where they won't be identified easily. What would it mean for the design of the IoT system that accounts for this privacy-seeking behavior?

Through this work, we seek to re-imagine an approach to privacy for smart workspaces that accounts for human behavior, is contextual, and is grounded in human-centered moral values, or the penumbra. Thus, we propose two theories of change:

1. Conceptualizing data and privacy in smart workspaces from a people-centric, place-centric, and data lens through a value-sensitive approach (section 3). We define People-centered in alignment with human-centered to emphasize empathy for building occupants. Unlike the word human which reduces them to purely anatomical beings, the word 'people' is more apt to capture the messiness of people's lives. Place-centered, in this context, does not mean geographical location or the physicality of a space. It has a phenomenological interpretation of how a particular space is used, what are the associated social meanings, cultural notions, the relationships held by its occupants, appropriate behavior, etc. (Harrison & Dourish, 1996). This meaning is what forms memories, associations, and communities for individuals.
2. Integrating these factors at the outset of creators' innovation processes, including architects, engineers, technologists, building managers, etc. to offer timely accommodations to shape privacy holistically (section 5).

Based on our theories of change, we conducted primary research through interviews, design probes, and a workshop. As a result, we introduce seven principles, 14 values, and a toolkit for privacy in smart workspaces (section 5). Together, these provide a structure to simultaneously consider people, place, and data for privacy. We propose this toolkit as a supplementary resource for multidisciplinary creators of smart workspaces. It is meant to enhance existing privacy practices, such as legal requirements and software innovations, rather than replace them.

The words umbra and penumbra used in this paper are derived from phenomena of light, respectively representing distinct and softer shadows of an object. In 1916, Supreme Court Justice William O'Douglas used the word 'penumbra' metaphorically to highlight that the right to privacy, even if not explicit, was implicit in other rights (Griswold v. Connecticut, Supreme Court of United States, 1916). We draw inspiration from this to expand beyond current privacy narratives (umbra) to advocate for a broader, human-centered approach (penumbra). Our goal is to acknowledge the co-existence of both and affirm that the proposed approach is meant to complement the existing ones.

2. The umbra of data privacy

The current privacy practices can be broadly categorized into 3 approaches (table 1): i) bringing transparency to existing data practices, ii) data management, iii) creating stand-alone technological solutions to empower end-users to protect themselves. These categories collectively define the 'umbra' of privacy approaches and suffer from numerous limitations. For example, the practice of notifying users about cookie collection on websites is mandated by the Fair Information Practice Principles (FIPPs) called 'Notice and Consent'. According to this principle, agencies must inform users about the specific reason for collecting their Personally Identifiable Information (PII), and that they "only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice" (IAPP Resource Center). While the intention of notifying individuals and laying the foundation for recourse is commendable, it does not give people any real agency at the time of accessing a digital service. In its current form, this principle is reduced to a mere checkbox to meet regulatory requirements and reflects a procedural approach to maximizing control rather than individual or societal welfare (Cate, 2006). Additionally, given the number of digital interactions today, it is virtually impossible for people to pay attention to the nuances of privacy policies conveyed in any form (McDonald & Cranor, 2008).

In the context of smart buildings, we found two most commonly used privacy practices: 'Notice and Consent', and 'de-identification of PII' of building occupants. However, as previously discussed, notice and consent have inherent limitations. De-identification, on the other hand, is designed to protect an individual's identity by reducing the number of identifiers. It seems promising in theory but fails in practice, especially when data from a large number of datasets is aggregated and because a sufficient level of data quality needs to be maintained for most use cases (Narayanan & Felten, 2014, p.2). Even when used together, these practices have a narrow focus, yet, they are most often used to slap on a privacy-preserving tag for smart buildings. Additionally, these practices overlook the qualitative narrative behind the data, which is paramount to privacy considerations in a physical space.

Table 1 Categories of current data privacy practices.

No.	Approach	Example	Limitation
1	Bringing transparency to existing practices (through usability, better notices etc.)	Fair Information Practice Principle (FIPP) of Notice and Consent	Doesn't urge for privacy as a preliminary and proactive consideration
2	Managing data (through policy, regulation, organizational strategy or technological solutions)	De-identification of Personally Identifiable Information (PII)	Not focused on the qualitative narrative behind the data
3	Creating stand-alone technological solutions to empower end-users	Privacy-enhancing technologies or PETs like Zero-knowledge Proof (ZKP)	Not widely known and often requires extra effort on their part

3. Defining the penumbra of data privacy

3.1 People, place, and data

To incorporate the qualitative narrative of data in a physical space, we first push against the narrative of buildings as computers. This narrative establishes smart buildings, including smart workspaces, as a topic of engineering prowess and building management. It overlooks their significance as the settings where human experiences and behaviors unfold, and, thus, labeling them as computers fails to capture their complexity and richness (Mattern, 2021). Additionally, most such interventions ignore the discussion around the context for which the 'smart' intervention is being designed (Desjardins, 2019), flattening out the nuances of contextually relevant behaviors. For example, privacy in a non-domestic realm like a workspace is a dialectic process of withdrawing and coming together (Altman, 1975). This dialectic process may be unavoidable, or sometimes even desirable to seek privacy, and is something to bear in mind when transforming workspaces into 'smart' environments.

In smart environments, the Internet of Things (IoT) embodies these lived experiences of the people through data. The data and algorithms that make IoT applications possible, "weave in the digital systems into the everyday fabric of society and create an environment in which people and technology become enmeshed" (Kemp, Jensen, Heath, 2020, p.1). The data gathered in these spaces encapsulates the inhabitants' experiences, behaviors, values, and ways of being, all deeply rooted within that context. Beyond mere numbers, it represents the qualitative aspects of these settings (Loukissas, 2019). To illustrate a simple example in the context of a smart workspace, peers may choose to stay after hours to work or to engage socially if such behavior aligns with organizational norms. This granularity of acceptable behavioral norms cannot be portrayed by data in a strictly algorithmic sense, underscoring the need to complement a computing-focused

perspective on data with a socio-behavioral one. Consequently, the digital transformation of workspaces into smart environments cannot be isolated from the socio-cultural and behavioral dimensions of human life. By extension, data and privacy in smart workspaces cannot be seen in isolation from the people and place with which it is bound. Therefore, we argue that conceptualizing privacy in smart buildings requires a multifaceted approach encompassing a people-centric, place-centric, and computing lens simultaneously.

3.2 Hypothesis and strategy

We observed that technical teams primarily led most smart workspace initiatives, with no to minimal engagement from a diverse array of stakeholders like architects, designers, and building managers. Each of these stakeholders has a unique focus in smart workspace projects, but the ultimate outcome is a cumulative product of their collective decisions, including those impacting privacy. To materialize our proposal for a comprehensive privacy approach encompassing people, place, and technical perspectives, we hypothesize that fostering multidisciplinary dialogue among these professionals is imperative. We assert that privacy is a shared responsibility and not just the purview of privacy engineers, and advocate for a collaborative endeavor involving architects, designers, various engineering specialists (including IoT engineers, developers, and privacy engineers), building managers, and owners. In this paper, we refer to this collective group of contributors as "creators." Together, these creators can integrate privacy values right from the initial stages of design and development, leveraging their distinct expertise, whether focused on human interactions, building management, or technical intricacies.

We also hypothesize that embedding people-centric and place-centric privacy considerations at the initial stages of the innovation process would empower the smart workspace creators to accommodate privacy concerns proactively. This proactive approach to privacy aligns with two of the seven Privacy by Design (PbD) principles proposed by Dr. Ann Cavoukian: i) proactive not reactive, preventative not remedial, ii) privacy embedded into design (Cavoukian, 2009). Our distinct contribution lies in emphasizing the creators' process rather than solely the end result, diverging from the traditional PbD perspective. We focus on this process through a values-based approach informed by the Value Sensitive Design framework (VSD) developed by HCI scholars Batya Friedman and David G. Hendry in the 1990s. VSD advocates for the integration of moral human values early on and consistently throughout the technology creation process (Friedman & Hendry, 2019). The framework consists of three components: conceptual investigation, done through literature review; empirical investigation, done through primary research; and technical investigation, which is designing the technical details of a computing system. This approach supports and strengthens our hypothesis regarding the early integration of privacy considerations from multiple dimensions.

4. Research

4.1 Methodology

Based on our hypothesis, the proposed theory of change and value-sensitive design approach, our research question was “How might we integrate people-centered and place-centered privacy values in the design and development phase of creating smart workspaces? We segmented it into two sub-questions (table 2): 1) what privacy values must be considered, 2) how might these values be leveraged to create privacy-preserving smart buildings?

Table 2 Design Research objectives and respective activities.

Sub Question	Research Overview	Activities
"What values and principles must be embedded in the design of IOT for workspaces to ensure a people-centered and place-centered privacy perspective?"	Define privacy values and principles by exploring occupants' perspectives	1. Conduct interviews and synthesize insights
		2. Generate privacy values and principles that are people-centric and place-centric
"How might we leverage different privacy values to facilitate the creation of privacy-preserving interventions for smart buildings by interdisciplinary teams?"	Develop and test a value-based approach for creators	3. Create an ideation prompt aligned with the definition of privacy value
		4. Integrate privacy values into a generative design process
		5. Preliminary test of privacy values through a workshop
	Design a systematic and tangible structure for use	6. Make privacy values tangible through visual metaphors
		7. Develop Privacy toolkit comprising of principles, values and process

Our first sub-question aimed to integrate the socio-cultural elements of privacy, recognizing that the privacy values in a workspace are unique to this context and distinct from those in domestic or retail environments. It was imperative that we avoid assumptions or bias when determining which values are relevant, therefore, instead of theorizing values based on a literature review, we investigated a functional smart workspace. This involved understanding the occupants’ perspective on being in a ubiquitous sensing environment, using the insights to define relevant privacy values and subsequently creating a process to integrate these values in a generative process for creators. Essentially, this approach created a feedback loop between the impact of such interventions and the front end of the design and development phases. It gave rise to three research objectives outlined in table 2: 1) Explore occupants'

perspectives to define privacy values, 2) Create and test a value-based approach, 3) Design a systematic and tangible structure for use.

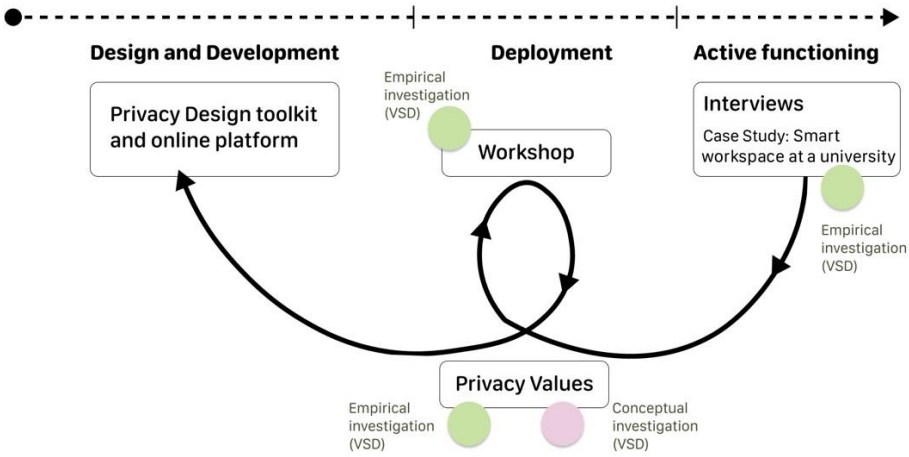

Figure 1 The research methodology was informed by value-sensitive design framework.

4.2 Participants

We examined a smart workspace on a university campus, equipped with "a ubiquitous sensing platform" (reference anonymized). The building serves as a workspace for students, researchers, faculty, administrative staff, and visitors who may occupy the common areas. Notably, it is home to students studying to be privacy specialists, a group that embodies dual identities: future privacy experts and occupants impacted by technology without having a voice in its implementation. They possess sound technical knowledge and might potentially shape similar innovations in the future. Yet, they navigate the space just like any other occupant, finding moments of laughter, relaxation, and celebration. The juxtaposition of their roles makes their insights invaluable for our study and presents an opportunity to positively influence how these future privacy specialists conceptualize privacy in similar contexts.

4.3 Defining privacy values and principles

We started with learning the goals of the smart workspace project on university campus by studying available documentation of the project. This secondary research laid the foundation to conduct primary research through silent observations of occupants' behaviors and seven one-on-one interviews, each including a design probe on Miro. The interviews started with broad questions about the participants' privacy mental model, followed by a reflection on their privacy-preserving behaviors in their workspace and, finally their perspective on the trade-offs between the interventions' benefits and risks. The insights from these interviews revealed that despite their robust technical knowledge, all participants felt unclear and uncomfortable with the continuous data sensing in their environment, and they all adjusted their behavior to achieve a sense of privacy, whether in response to the sensors or as a general practice. These behaviors ranged from avoiding personal phone conversations in most areas due to microphone sensors, to creating personal barriers such as headphones or leveraging physical barriers like doors. A participant mentioned:

> "…in Manhattan hiding in the crowd made it easier to share sensitive information even though I was aware that there were cameras everywhere…I'm more comfortable taking sensitive calls on (the street) during the workday than at (this building)." (Participant 8ZwXia)

We leveraged insights from these interviews to create a preliminary set of people-centered and place-centered privacy values. In line with VSD principles (Friedman & Hendry, 2019), we distinguished between the personal values of the occupants and the moral values relevant to creators at scale. The privacy values thus produced as a part of this research are moral values and complemented by a definition refined through four rounds of iteration. Wherever possible, we broke down a large concept into smaller and specific components. For example, we divided the need for transparency that all participants mentioned in one way or another into three values: (1) purpose and practice, (2) comprehension, and (3) perceptibility. Therefore, the need for transparency is a principle that encompasses these three values.

4.4 Developing and testing the approach

To ensure the practical integration of privacy values into the creation process, we first transformed each value's definition from a literal meaning into an ideation prompt using an action verb such as 'specify', 'provide', 'explain' etc. This approach draws inspiration from generative design processes and postulates that answering these prompts can spark ideation (Desjardins, 2019) for engineers, designers, and architects and encourage innovative perspectives on data and privacy right from the initial stages of their design. For example, the value of 'perceptibility' is defined as 'bring awareness to the hidden or less obvious presence of data sensing.' This can be addressed by architects through a decision to place the sensors visibly at an eye level, or by engineers by designing an app that notifies occupants when they are in the vicinity of sensors.

The finalized privacy values were tested through a generative design workshop involving the same six participants. They were paired and guided through a systematic process to generate IoT ideas for the building without initial priming toward privacy values. The workshop had three parts: first, participants assumed a 'User hat' to envision their own needs as occupants, then transitioned to a 'Creator hat' to refine ideas considering relevant stakeholders, necessary data, and privacy values, and finally, a group discussion to reflect on the process. The goal of the workshop was to facilitate a human-centered design process where the needs of users precede sensors and technology. Overall, the process touched on both aspects of their unique identity: the occupants impacted by the IoT intervention and privacy engineers who might work on similar interventions in the future.

The workshop had two significant findings. Firstly, introducing a broader perspective shifted the privacy dialogue from the conventional data management and software-centric approaches toward a human-centered approach that fostered greater empathy among participants. It opened them up to visualizing the people whose data is being collected and processed. A participant said:

> "…we think about data in the context of a company all the time, but some organization would probably be managing data for a building which is much more in the face of people actually using the building on a day-to-day and I felt like this gave us a different perspective on how to think about what we are collecting." (Participant kDiWCB)

Secondly, it became evident that despite the success of a human-centered approach, participants struggled to effectively leverage the values to refine their ideas. For example, some found it difficult to pick values relevant to their idea, while others struggled with the abstract nature of these values and found them relatable only with tangible examples during the group discussion. This realization underscored the necessity for a formal design exercise to enhance the tangibility of privacy values in a refined process.

4.5 Visual metaphors for privacy values

We identified two crucial aspects requiring resolution to enhance the tangibility and approachability of privacy values. Firstly, the overall process required refinement. Secondly, our reflections as workshop facilitators highlighted that the vocabularies and mental models concerning the application of these values varied widely across professional disciplines. For instance, the prompt of creating barriers to allow occupants to disconnect from data collection could manifest as physical screens, laptop camera covers, or software interventions like VPN, depending on the disciplinary perspectives. We wanted to bring out all these perspectives irrespective of the differences in vocabulary and mental models across disciplines.

To bridge this mental model gap, we proposed using a unique metaphor for each privacy value through a visual representation. Metaphors are commonly used in design practice for idea generation, but most importantly, they can transcend the boundaries of professional disciplinary knowledge (Saffer, 2005). They allow 'cross-domain mapping" by taking familiar ideas, objects, and experiences and "recasting them onto unknown or abstract concepts to give them structure and meaning" (Erickson, 1995; Lockton, 2013). Therefore, employing metaphors would allow the values to resonate with a broad interdisciplinary audience while simultaneously leaving room for leveraging their individual knowledge. For example, the value of *Perceptibility* for bringing awareness to the less obvious presence of data sensing could be represented using 'Waldo' from Where's Waldo. Waldo is a western character hidden in plain sight in a crowd but is noticeable due to his distinct manner of clothing and hair. The visual depiction spotlighting Waldo conveys the message of drawing attention to something camouflaged in plain sight. It can empower interdisciplinary creativity while establishing a shared understanding of the privacy value.

The integration of visual metaphors alongside their definitions led to the creation of a card format, resulting in a comprehensive deck of 14 cards that underpins the toolkit's ideation process. To make the value cards usable by creators, we color-coded as per three broad phases of the design process: Conceptualizing (yellow), Detailing (blue) and Refining (orange).

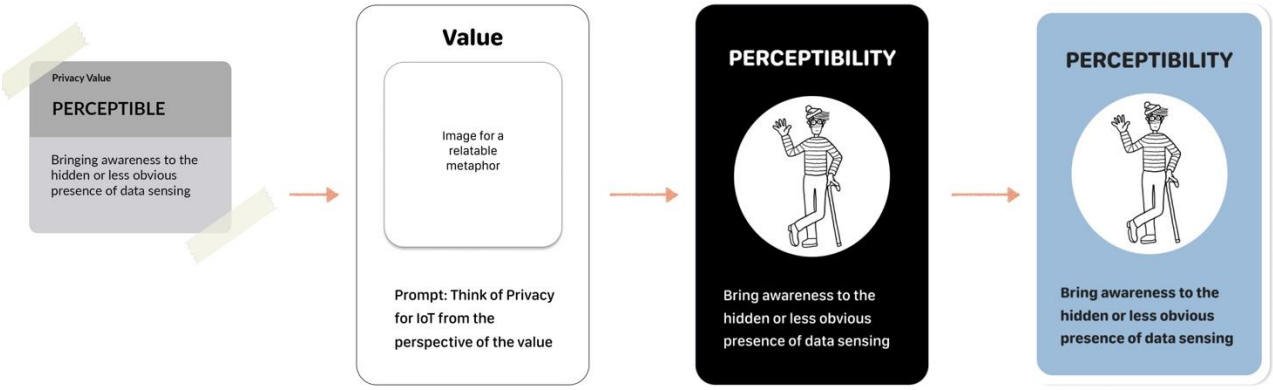

Figure 2 The visual design of privacy values evolved from tiles with title and definition to cards with title, definition and a visual metaphor.

5. Privacy toolkit

We propose a 'Designing with Privacy' toolkit for smart workspaces to be used in a multidisciplinary capacity by stakeholders like architects, designers, IoT engineers, privacy professionals, building managers etc. We recommend that the toolkit is introduced early in the design and development phases to foster privacy ideation. This timing is crucial due to the interdisciplinary nature of the approach, as decisions made during the early phases of design and construction have a far-reaching impact. They can be challenging and/or expensive to change post-implementation. Consider the scenario from section 4.4, if an architect proposes to place all sensors at or below eye level to enhance their perceptibility, she would have to plan for the exact placement in her design. This decision would become an important part of her design brief since it is linked with the electrical planning as well as the interior aesthetics. On the other hand, a software-centric endeavor to develop an app that notifies the occupants in the vicinity of sensors may be implemented down the road but would still need resource allocation. To make these considerations tangible, the toolkit culminates in the creation of a one-page privacy brief, collaboratively developed and agreed upon by the team of creators. The privacy brief serves as an essential component of the project goals incorporating privacy considerations from the outset instead of an afterthought.

5.1 Format and content

The toolkit is a downloadable PDF available at https://tinyurl.com/privacyforIoTtoolkit. It contains

- 7 core principles color-coded as per three stages of the process: conceptualizing (yellow), detailing (blue), and refining (orange) (figure 3),
- 14 privacy value cards framed as ideation prompts,
- Guidance on how to prepare and use the toolkit,
- Worksheets for scoping and ideation,
- Privacy brief preparation based on multi-disciplinary team's ideas and prioritization.

	Principle	Value	Prompt
CONCEPTUALIZING	Bring in the voice of occupants/ end users	Empathy	Be sensitive to the needs and perspectives of those implicated by the system
		Participation	Engage multiple stakeholder groups throughout the decision making process
	Create IoT interventions that are specific to building use and place	Contextual	Design details based on the needs of users of this environment
		Culturally Situated	Account for the appropriate cultural values and norms
DETAILING	Distinguish between Public and Private areas of the building based on occupant behavior	Differentiate	Distinguish between data practices for public v/s private areas of the building
	Enable Transparency for the occupants/ end users	Purpose and Practice	Clearly specify the purpose of data collection and data use practices
		Comprehension	Explain purpose, practices and choices in a manner that users understand
		Perceptibility	Bring awareness to the hidden or less obvious presence of data sensing
	Give Agency to the occupants/ End users	Barriers	Allow users to temporarily disconnect themselves from the IoT system
		Adaptation	Enable users to adapt the IoT system to reflect their preferences
		Accessible	Provide access to resources (person or other) for help and/or questions
REFINING	Assess and evaluate to find the right balance between intent and impact	Equilibrium	List the benefits and potential/ likely risks to find the right balance
		Foresight	Consider the impact of IoT system on users and/or society over time
	Take responsibility for outcomes and comply with measures to address concerns.	Accountability	Create mechanisms for ensuring compliance and addressing user concern

Figure 3 Privacy principles and the associated values color-coded as per three stages of the innovation process for smart workspaces: conceptualizing, detailing, and refining.

The pdf format of the toolkit offers flexibility for the participants to use it digitally or in a printed letter-sized landscape format, depending on the preferences and location of the participants. It can be used one of two ways: (1) individuals can fill it out as a workbook when working alone or asynchronously with a team. Following this individual exploration, team members should collectively discuss and synthesize their ideas, culminating in the creation of a cohesive privacy brief. (2) In-person teams can conduct a generative workshop with a facilitator. The facilitator prepares for the session by printing the prompt cards (so that the teams can move them around as they brainstorm), the table of values and principles (figure 3) for reference, a scoping worksheet, and a copy of the design brief, both of which are intended to be collectively filled out by the team. With these materials, the facilitator would guide the team with step-by-step instructions. Whenever possible, the facilitator should help in sharing copies of the finalized privacy brief with all team members.

5.2 Guidance for using the toolkit

Our instructions for using the toolkit are intentionally concise, allowing flexibility for diverse disciplinary stakeholders. This stems from our recognition that processes during the early stages of the project could vary for each disciplinary stakeholder and need in-depth investigation beyond the scope of this research. Thus, we aimed to avoid imposing rigid guidelines and ensure that the toolkit is a useful starting point for privacy ideation rather than a prescriptive framework. Consequently, the instructions focus on two key aspects:

1. Ideal time for utilization: The toolkit is most impactful at the project's conceptual stage when all details are in a nascent form, but we recommend that the team members re-visit it periodically for reflection and re-imagination, particularly during critical decision-making points.
2. Scoping from a human-centered perspective: Prior to ideation, the creators are prompted to scope the project by considering the occupants and their needs, as well as the collaborators involved in the project. The goal is that the team reflects on individuals affected by the technologies and grants an equal voice to all stakeholders in the ideation process. We anticipate a discussion amongst the collaborators in the creation of this scope, thereby creating alignment before the brainstorming phase. Questions like ‘who will permanently occupy this space?’ ‘in what activities would they engage in this space?’ are vital aspects we hope are discussed.

We have also incorporated four ideation tips drawn from the first author’s experience as a facilitator in generative design workshops. One of the key tips is 'Commitment over right answer’, reinforcing the importance of iteration and refinement of ideas as the project progresses.

5.3 Ideation worksheets

The toolkit includes worksheets designed to facilitate ideation for 2-4 values at a time (figure 4). This deliberate choice aims to prevent overwhelming participants with all values all at once and enable thoughtful consideration of multiple factors in greater depth. Participants can express their ideas through drawings or written descriptions. This phase mirrors the diverging phase in the double diamond design process. After generating ideas for each or selected values, the team should prioritize the most relevant ones.

When used by a team, we advise that the ideation should be an individual endeavor before everyone comes together for a joint discussion. The collective discussion provides the space where ideas can be openly shared, debated, and prioritized, fostering a thorough exploration of various perspectives before finalizing decisions. Notably, the toolkit refrains from imposing predefined metrics for prioritization to steer clear of a one-size-fits-all approach. Instead, we hope that the teams are empowered to devise metrics tailored to their specific project needs to lead to the final step of developing the privacy brief.

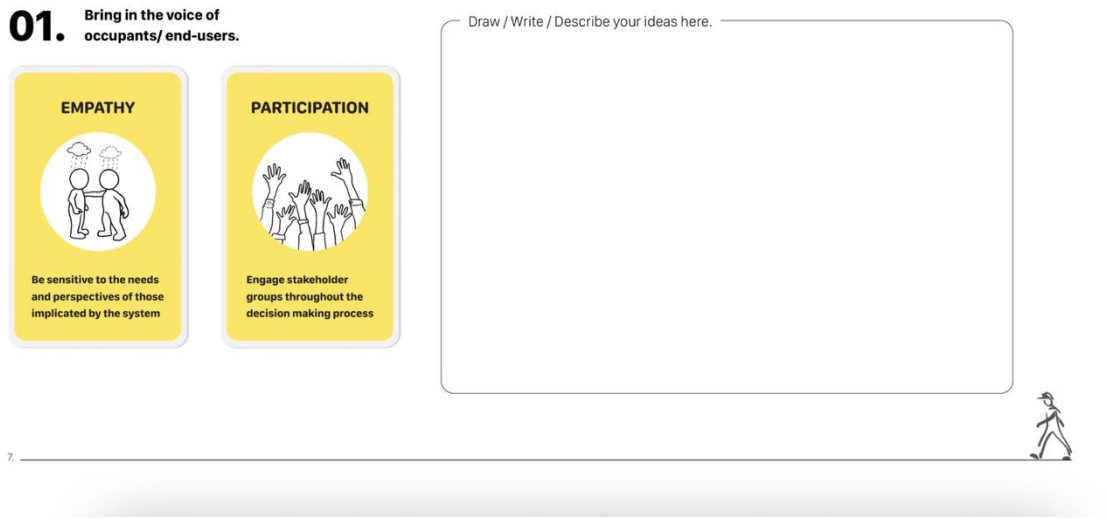

Figure 4 Ideation worksheets with 3-4 privacy values and space for ideation.

5.4 Privacy brief

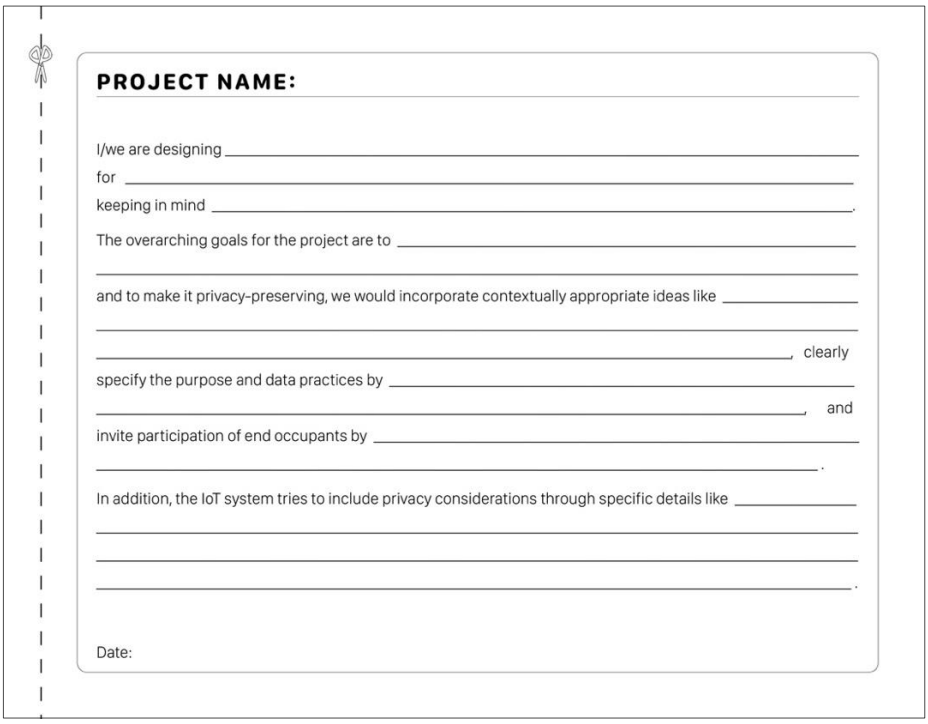

Figure 5 Privacy Brief to be created and endorsed collectively by the team.

The privacy brief is a one-page summary outlining the scope and the team's or individual's privacy-preserving vision for the project (figure 5). When used by a team, it is collaboratively completed at the conclusion of the toolkit use, with each team member retaining a copy. The brief includes the team (or individual) endorsement to instill a sense of ownership, accountability, and a meaningful commitment within the team. It also functions as a concrete artifact, making the team's prioritized values and ideas explicit for all stakeholders.

For the structure of the brief, we deliberately chose to include two privacy values as essential components: purpose and practice, and participation. We retained 'Purpose and Practice' due to its integral role in existing data privacy practices and identified 'Participation' as a significant omission in numerous smart building and smart city initiatives. Meanwhile, the rest of the brief provides room for incorporating other privacy values and related ideas prioritized by the team. Much like project briefs evolve, we hope that this privacy brief is refined over the course of the project, with its various iterations serving as valuable project documentation.

6. Discussion and future work

We aimed to go beyond the status quo of current privacy practices, or the umbra, and create a broader approach for privacy in smart workspaces based on human-centered experience and values, or the penumbra. To do this, we propose a theory of change that intertwines data, people, and place in smart workspaces through a value-sensitive design lens. During our research, we studied the work of scholars who advocate for the qualitative aspects of data; including anthropologists like Genevieve Bell and Tricia Wang, academics and authors like Yanni A. Loukissas, data feminists like Catherine D'Ignazio & Lauren Klein, information designers like Giorgia Lupi, and interaction design researcher like Audrey Desjardins. We also studied smart building and smart city initiatives which amass large amounts of occupant data in the name of infrastructure management and view data solely as a quantitative metric. We didn't come across any approach in this realm that addresses the co-existence of this dual perspective on data and attempts to bridge it. Although our work is focused on privacy, we hope that it also fills a gap in seeing data from a dual perspective.

We have laid a foundation for the privacy discourse in smart spaces, but we acknowledge the necessity for continuous refinement and expansion through meaningful partnerships. To take this initiative forward, the first author is seeking collaborators for two future projects. The first project involves testing and refining the toolkit with a wide group of audience to ensure its effectiveness. The second project is the creation of a comprehensive 'Designing with Privacy' platform. The platform is envisioned to be the central hub for accessing the toolkit along with three additional features:

1. **Real-time collaboration**: The platform will be interoperable with whiteboard tools like Mural or Miro to enable real-time collaboration among remote teams. This feature will also help in creating living documents for the projects and allow teams to revisit and refine their privacy brief as needed.
2. **Resource Repository**: Community members can upload and share implemented ideas generated from the toolkit. Therefore, the platform acts as a valuable knowledge repository, containing both successful strategies and insights gleaned from the relevant challenges.
3. **Community Hub**: The platform provides space for professionals to connect, and engage in creative discussions and collaborative endeavors.

Together, these three features would elevate the utility of the privacy principles and values developed through this research, potentially fostering an alternative privacy narrative privacy within a broader community. We also hope that this serves as a scaffold to enable the creation of privacy values relevant to other contexts like smart homes. Figure 6 illustrates an early prototype of the platform.

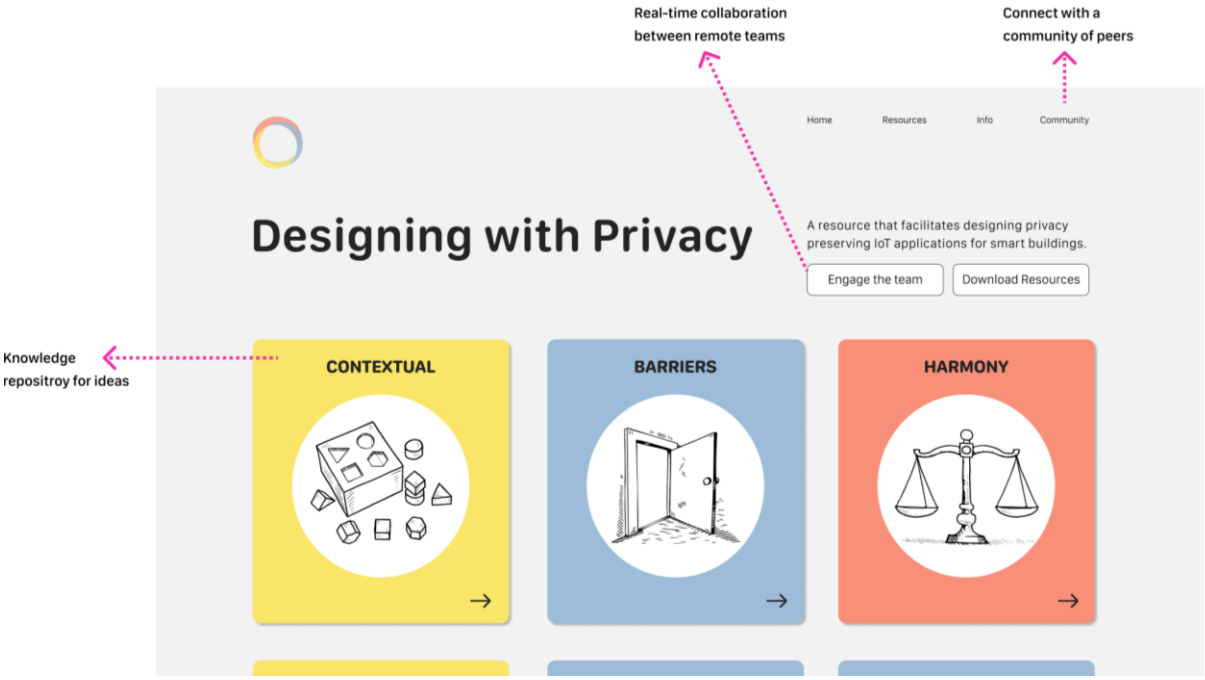

Figure 6 Ideation worksheets with 3-4 privacy values and space for ideation.

7. Conclusion

We conducted the research in three parts, first, we interviewed the occupants of an existing smart workspace to synthesize relevant privacy values. Next, we conducted a workshop to test how these values could be integrated with a creator's process. Finally, we used the learnings from the workshop to develop a tangible structure for creators in the form of a privacy toolkit. The research emphasized that shifting the privacy conversation from software and data management approaches, to one focused on people and place at the front end of the design process, generated greater empathy in creators. This human-centered perspective also relieved them of the pessimism around technology and provided hope that early deliberation in the innovation process can reduce the burden for 'fixing' technology after the fact.

The body of work produced through this research includes seven privacy principles, a deck of fourteen privacy value cards, and a privacy toolkit for applying these in practice for smart workspaces. These tools are designed to complement the existing processes of multi-disciplinary professionals, offering timely accommodations and enriching the workflow without replacing established methods. This work lays the foundation for what we hope is a larger body of work on privacy discourse for smart buildings.

Acknowledgements: This work has been made possible with the support of CyLab at Carnegie Mellon University, and the invaluable contributions of the research participants.

8. References

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding* (First Printing ed.). Brooks/Cole Publishing Co.

Cate, F. H. (2006). The Failure of Fair Information Practice Principles. *Consumer Protection in the Age of the Information Economy*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972#

Cavoukian, A. (2022). *Privacy by Design: Take the Challenge*. Information and Privacy Commissioner of Ontario.

Coles-Kemp, L., Jensen, R. B., & Heath, C. P. R. (2020). Too Much Information: Questioning Security in a Post-Digital Society. *In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376214

Desjardins, A., Viny, J. E., Key, C., & Johnston, N. (2019). Alternative Avenues for IoT: Designing with Non-Stereotypical Homes. *In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, (CHI '19). Association for Computing Machinery, New York, NY, USA, Paper 351, 1–13. https://dl.acm.org/doi/abs/10.1145/3290605.3300581

Erickson, T. D. (1995). Working with Interface Metaphors. *Readings in Human–Computer Interaction (second ed.)*, (pp. 147–151). https://doi.org/10.1016/B978-0-08-051574-8.50018-2

Friedman, B. (1997). Human values and the design of computer technology (ed.). CSLI Publications.

Friedman, B., & Hendry, D. G. (2019). *Value Sensitive Design: Shaping Technology with Moral Imagination* (Illustrated ed.). The MIT Press.

Greenfield, A. (2006). Everyware: *The Dawning Age of Ubiquitous Computing* (first edition). New Riders Publishing.

Harrison, S., & Dourish, P. (1996). Re-place-ing space. *In Proceedings of the 1996 ACM conference on Computer supported cooperative work (CSCW '96).* Association for Computing Machinery, New York, NY, USA, 67–76. https://doi.org/10.1145/240080.240193

International Association of Privacy Professionals

Lockton, D. (2013). Design with intent: a design pattern toolkit for environmental and social behaviour change (Doctoral dissertation ed.). *Brunel University School of Engineering and Design PhD Theses.*

Loukissas, Y. A. (2019). *All Data Are Local: Thinking Critically in a Data-Driven Society* (Illustrated ed.). The MIT Press. https://doi.org/10.7551/mitpress/11543.001.0001

Mattern, S. (2021). A City Is Not a Computer: Other Urban Intelligences. Princeton University Press.

McDonald, A. M., & Cranor, L. F. (2008). The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society, vol. 4, no. (3) (2008), 543-568.*

Narayanan, A. & Felten E.W. (2014). No silver bullet: De-identification still doesn't work. *Freedom to Tinker, hosted by Princeton's Center for Information Technology Policy.* https://www.cs.princeton.edu/~arvindn/publications/no-silver-bullet-de-identification.pdf

Saffer, D. (2005). The Role of Metaphor In Interaction Design (Master's thesis ed.). *Carnegie Mellon University*.

About the Authors:

Isha Hans is currently a visiting lecturer at University of Waterloo's Stratford School of Interaction Design and Business. Her work focusses on bringing insights from human behavior upfront for technologically complex innovations, including privacy and cybersecurity.

Dina El-Zanfaly is a computational design and interaction researcher. She was recently named the Nierenberg Assistant Professor of Design in the School of Design at Carnegie Mellon University (CMU). She directs her newly founded research lab, hyperSENSE: Embodied Computations Lab.

Lorrie Cranor is a Professor of Computer Science, and Engineering and Public Policy at Carnegie Mellon University. She directs CyLab Usable Privacy and Security Laboratory (CUPS), dedicated to enhancing the usability of privacy and security technologies through research and development.