

# PENUMBRA OF PRIVACY

DESIGNING WITH PEOPLE-CENTERED  
AND PLACE-CENTERED PRIVACY VALUES  
IN SHARED SMART WORKSPACES



Received the Kynamatrix Research Network  
"Innovation through Collaboration" 2021 Grant Award.

Received School of Design Merit Award, 2022.

# PENUMBRA OF PRIVACY

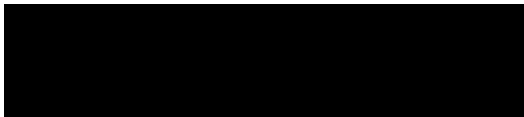
DESIGNING WITH PEOPLE-CENTERED AND PLACE-CENTERED  
PRIVACY VALUES IN SHARED SMART WORKSPACES

A thesis submitted to the School of Design, Carnegie Mellon University, for  
the degree of Master of Design in Design for Interactions in May 2022.



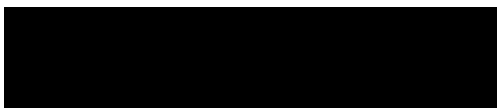
---

Isha Hans, Author



---

Dina El-Zanfaly, Advisor



---

Lorrie Faith Cranor, Advisor

*"It is increasingly necessary to be able to think of new technologies in different ways, and to be critical of them, in order to meaningfully participate in that shaping and directing."*

- James Bridle (New Dark Age: Technology and the End of the Future, 2018)



**ABSTRACT**

The current digital privacy practices have proven to be insufficient. They have evolved as a reactionary response to the growing concerns instead of being a consideration from the start. Despite being insufficient, these practices have set the status quo for most emerging technologies, including smart buildings, to adopt a purely computing perspective towards privacy. However, buildings and workspaces, whether smart or not, are not computers, but rather places where people's lives play out. Therefore, this thesis focuses on complementing the current privacy practices, or the umbra, with a broader approach based on human-centered experience and values, or the penumbra. A novel approach is proposed based on two re-framings: 1) combining a people-centric and place-centric perspective for privacy with a computing perspective, and 2) creating preventative approaches instead of remedial ones by embedding people-centric and place-centric privacy values in the front end of the design process for creators. These creators primarily include architects, engineers, designers and building managers.

The research was conducted in two parts: interviews with the occupants of an existing smart workspace to identify relevant privacy values, followed by a workshop to test how these values might be used in the process by creators. The research concluded that shifting the privacy conversation from software and data management approaches, to one focused on values at the front end of the design process, created greater empathy in creators. It helped them visualize the lived realities of people whose data is collected and processed in a place, and discuss new ideas. This investigation produced seven core principles and fourteen associated values for making privacy a preventive rather than a remedial approach in shared smart workspaces. Even though the principles and values were generated for shared smart workspaces, they are relevant for other shared contexts in the non-domestic realm, and may even be useful for the domestic context with critical reflection and adaptation. These principles and values have been made tangible and approachable for creators through three design outcomes: first: fourteen privacy value cards framed as ideation prompts, second: a privacy toolkit that integrates principles and prompts along with guidance on how to use them, third: a proposal for a platform for an interdisciplinary group of creators working together on smart building projects. In addition to these research and design outcomes, this work also contributes to the privacy discourse through a novel approach better suited for smart buildings.

## **ACKNOWLEDGMENTS**

First, I would like to thank my advisors, Dr. Dina El-Zanfaly and Dr. Lorrie Faith Cranor, who have supported me and trusted me in this journey. I have received immense support from both, not only for shaping this thesis but for life in general. Even when I decided to take a gap year from 2020 - 2021 and was technically not their advisee, their investment in my wellbeing and future helped me get through a difficult time in my life.

I'm grateful to Daragh Byrne, Dr. Molly Wright Steenson and Stacie Rohrbach for the constant support. The chats with them helped me zoom out from my own process and see things more clearly. I will also cherish all the little side notes in our conversation that made us laugh and take a break from our everyday lives.

I must also thank the new friends I have made through trans-disciplinary collaborations in the last year. Our conversations started with talking about privacy, but I'm glad that we got to know each other beyond the scope of our classes. I especially appreciate that we find the differences in our backgrounds and ideas mutually interesting.

I'm thankful to all my peers who have been on this roller coaster ride with me. Even though we were all working on our own theses and were going through our own ups and downs, we were connected. This friendship, support and feeling of belonging has meant a lot and I hope for it to always stay intact.

Last, but not the least, I'm indebted to my family who have walked this path with me in spirit and been a consistent anchor in my life.

# CONTENTS

Abstract

Acknowledgments

Preface

## ***PART I: THE PENUMBRA OF PRIVACY FOR SHARED SMART SPACES***

### **Chapter 1. Introduction**

- 1.1 Need and Significance
- 1.2 Research Objective
- 1.3 Research Methodology
- 1.4 Intended audience
- 1.5 Scope and Limitations
- 1.6 Areas of inquiry and thesis overview
- 1.7 Key definitions

### **Chapter 2. 'Smartification' of the Built Environment**

### **Chapter 3. Understanding Privacy**

- 3.1 A Computing lens, or 'Umbra' of Digital Privacy
- 3.2 A People-centric and Place-centric lens

### **Chapter 4. Creating 'Penumbra' of Privacy for Smart Workspaces**

## ***PART II: TOOLKIT DEVELOPMENT***

### **Chapter 5. Research Methodology**

- 5.1 Values-based approach
- 5.2 Case study

### **Chapter 6. Exploration, Generation and Iteration**

- 6.1 Need and Significance
- 6.2 Research Objective
- 6.3 Research Methodology
- 6.4 Intended audience
- 6.5 Scope and Limitations
- 6.6 Areas of inquiry and thesis overview

### **Chapter 7. Design Implementation**

- 7.1 Privacy Design Toolkit for shared Smart Workspaces
- 7.2 An online Platform for Designing with Privacy

## ***PART III: CONCLUDING REMARKS***

### **Chapter 8. Conclusion**

### **Chapter 9. Personal Reflection**

References

Appendices

## PREFACE

The word 'umbra' and 'penumbra' are derived from a phenomenon of light. When light falls on an object, it forms a dark shadow called the 'umbra' and a surrounding lighter shadow called the 'penumbra'. The umbra, being the darkest part, is clearly defined and most easily discernible, whereas the penumbra is softer with less clearly defined boundaries. Therefore the word 'penumbra' is used as a metaphor for concepts that may be ambiguous, or implied. In 1916, supreme court Justice William O'Douglas used it with respect to privacy to place emphasis on the fact that the right to privacy, even if not explicit, was implicit in other rights. He said:

*"...the specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance"*

- John Justice William O'Douglas (Griswold v. Connecticut, Supreme court of United states, 1916)

I am drawing inspiration from this to go beyond the status quo of current privacy practices, or the umbra, and highlight a broader approach based on human-centered experience and values, or the penumbra. The current practices are heavily skewed towards a software and data management related conversation, and my hope with broadening these is that they would strengthen the 'Preventive not Remedial' approach to privacy (Cavoukian, 2009). But, just like penumbra doesn't exist without the umbra, the proposed approach includes aspects of the current practices and is meant to complement them and not replace them.

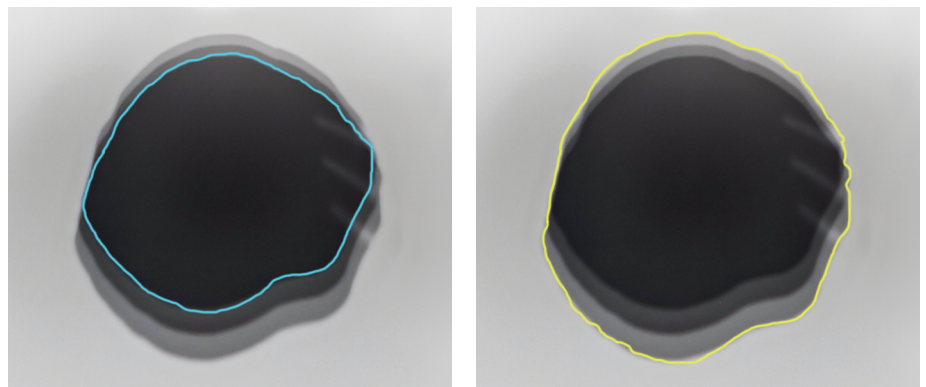


Fig 1. The darkest shadow, called the Umbra (left), the lighter fuzzy shadow called the Penumbra (right)

## MOTIVATION AND POSTURE

### Trans-disciplinary allegiances

The choice of this thesis topic was influenced by two factors: my background as an Architect and the exposure to technological topics at Carnegie Mellon University. For 5.5 years before coming to CMU, I practiced as an Architect and taught across different architecture schools in Mumbai. During that journey it became clear to me that the future of the built environment is becoming more and more intertwined with technology. 'Smart cities' and 'smart buildings' had started becoming a buzz yet it was unclear how they were better beyond the operational efficiencies they brought in, or how they integrated a process to understand the lived realities of people. I had been taught an architectural process that started with understanding the people I was designing for, through ethnography, field research, conversations and climate considerations. Learning about people, their activities, experiences, expectations and life in general was always the first step before any ideas were put to paper. Yet, suddenly, the built environment got reduced to a mere topic of engineering and managing infrastructure capabilities. While I acknowledge that it is a valuable line of inquiry, I also couldn't stop wondering about the experience of the people who occupy these environments.

Coming to CMU with these thoughts at the back of my mind inspired me to complement my learnings about human-centered design with learnings about technology: in terms of its outcomes, its capabilities as well as the process that shapes it. I got exposed to the topic of data privacy in my very first semester and the more I learnt, the more it intrigued me. Including this thesis, I have spent about three years understanding its different facets. In addition, I have explored privacy concepts through numerous conversations and five projects that are not included in this document but can be found on my website ([ishahans.com](http://ishahans.com)). Through my conversations with fellow designers, architects, technologists, future policy makers and business professionals, I could see the gaps in different disciplinary perspectives and the scales at which the impact is conceived. My non-designer friends asked 'What has privacy got to do with Design?', my design friends wondered whether I was trying to do 'experience design' or 'product design' or 'service design' or another kind of design. My design research friends were concerned about the boundaries between exploratory, generative and evaluative research and my engineer friends probably squinted their eye wondering what were my technical skills to contribute to this topic and whether this study is going to be statistically significant to be useful.

Needless to say, trying to answer these questions helped me stitch the seemingly disparate pieces of my research into a coherent body of work. But most importantly, this process helped me embrace my identity as an interdisciplinary thinker. In the podcast on Data Materiality hosted by Vasari Research Centre for Art and Technology, Yanni Loukissas talks about his multiple allegiances: as a Designer and a scholar, as a Greek and an American, as a Designer and as an Ethnographer. He speaks about the multiplicity of identities depending on how they are received by others and the feeling of being an outsider everywhere. Reflecting on his experiences gave me a fresh perspective to think about the dualities in my multiple little worlds. With one foot in understanding the mechanics of digital privacy and the other in how to ask critical questions about technology keeping people at the center, I often find myself on the fringe of the two. This position comes with its own challenges but also serves as a bridge to connect the dots between very different schools of thought: in this case a technical one, an STS (Science, Technology, and Society), one and the human-centered design one. Hence, this body of work is shaped by my experience as a spatial experience designer, my concern for the future of the built environment, my beliefs as a human-centered designer and my understanding of digital privacy.

### **Contextual and Situated perspective on Data**

In his book 'All Data are Local', Yanni Loukissas argues that data is neither heterogeneous nor universal. This has also been argued by feminist scholars in science and technology Catherine D'Ignazio & Lauren Klein in their book Data Feminism and by Genevieve Bell, an anthropologist working at the intersection of cultural practice and technological development, in her famous talk 'The Secret Life of Big Data'. Further, Yanni cautions us to not give into the temptation to aggregate data or Digital Universalism, because the data is not place-less. He contrasts Nicholas Negroponte's argument that 'being digital means less and less reliance on a particular place' by arguing that the setting matters because data is deeply entangled with the communities, places, histories and ways of knowing. The respective values and assumptions are embedded in how and where data is created, when it is created (that is data are alleged claim, Borgman, 2015), what data is captured and how it is interpreted. This is somewhat the opposite of big data which tends to flatten out the nuances of the stories that data tells in an attempt to make it more generic and applicable at scale. I deeply resonate with the situated framing of data where the meanings derived from data are not stripped off its context. Tricia Wang, an anthropologist, popularized this framing of data as 'Thick Data', which gives a rich context to data through stories.

All the above ideas have influenced a key choice in this research, that is grounding with respect to shared smart spaces, and a specific one at that: smart workplaces. Some of the values generated as a part of this thesis are more directly applicable to a workspace context than a smart home context, but may be applicable to other shared contexts in the non-domestic realm with critical reflection and adaptation.

### **Balance and Precedent setting**

A piece of technology by itself is neither absolutely beneficial or absolutely harmful, just like a kitchen knife by itself is a tool that can be used for chopping or to inflict harm. What ascribes a beneficial or harmful quality to technology is a cumulative outcome of the respective decisions made by the makers and the surrounding conditions that enable, disable or motivate its use. Similarly, the Internet of Things, and therefore data and privacy, are double edged swords. Neither of them is good or evil in itself, and often involves tradeoffs and a need to find the right balance. This interest in finding a balance between the meaningful use of data and the vulnerabilities associated with its abuse has shaped my research in its current form. For example, the design probes used during the interviews were created with a goal of finding the threshold between the perceived benefits of IoT and the associated privacy risks in a smart workspace on CMU campus.

Decisions around technology set the precedents for the world we create and subsequently get shaped by it. Therefore the decisions made by designers or technologists cannot be seen in isolation from each other, as is usually the case in siloed practices.

*PART I: THE PENUMBRA OF PRIVACY  
FOR SHARED SMART SPACES*

CHAPTER 1.  
**INTRODUCTION**



## 1.1 NEED AND SIGNIFICANCE

Data is rapidly becoming the most valued asset of the 21st century (Harari, 2018). In the context of buildings and cities, it is expected to help make the built environment operationally efficient and easy to manage (Eric, 2019). There is an inherent trade-off between this value proposition and the privacy of the individuals in these spaces whose data is collected, aggregated, inferred and disseminated. This trade-off is often tipped in favor of extensive amounts of data collection and inferencing, whether advertently or inadvertently. The issues surrounding data practices have garnered attention and concern in the last two decades, and it is undeniable that some of the current tactics are making substantial contributions. The current tactics either revolve around data protection and management (through policy and regulation, and organizational strategy), or bringing transparency to existing practices (through notices, usability etc.) or creating stand alone technological solutions for empowering end-users to protect them from existing undesirable practices on the internet (also called Privacy Tech). However, most of these approaches have evolved as a reactionary response to growing privacy concerns on the internet and are not well suited to the critical questions of what should or should not be done in the context of rather new applications of technology like Internet of Things (IoT) and their applications for buildings (Greenfield, 2006). For example, giving notice about video surveillance in a space is helpful for the occupants but does not strike at the root of the problem of asking critical questions about the use of this technology and the related data practices. Additionally, current privacy approaches are rarely designed with an interdisciplinary purview, for example for the engineers, designers, architects, building managers etc. who all play a part in shaping smart buildings. Therefore the current practices are insufficient in their direct transference to IoT and their applications for making buildings smart. Despite proving insufficient, they have set the status quo, or 'umbra', for conceptualizing privacy for smart buildings. I argue that this is not a good replicable model for two reasons:

1. IoT by its very nature connects a large number of data points with each other and provides a greater aggregated surface for interception. This increases privacy risks for occupants and the responsibility to be more thoughtful.
2. Most importantly, buildings, and cities, are not computers (Mattern, 2021), but places where human life plays out. IoT in the context of smart buildings is about much more than just the sensors. It is an instrument that embodies the lived experiences of the people in a physical space through data. This data and the algorithms needed to make these applications possible, 'weave in 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).

## 1.2 RESEARCH OBJECTIVE

This thesis argues for the need for broader approaches, or defining the penumbras, to the current privacy practices of the creators of smart buildings. The digital aspects of privacy in smart buildings cannot be seen in isolation from the human side of things because just like any other technology, IoT in the built environment is deeply intertwined with the human experience, behavior and values. (Friedman, 1997). For example, in the context of a workspace, most people tend to not share too much about their personal life and take private calls either in a secluded area where they may not be overheard or in more public areas where they cannot be identified easily. What would it mean for the design of the IoT system that accounts for this privacy-seeking behavior? It is important that the interdisciplinary team of creators behind smart building projects proactively account for the human experience and values in thinking about data and privacy. As James Bridle has stated in the context of technology and data:

*"A new shorthand is required, one that simultaneously acknowledges and addresses the reality of a world in which people, politics, culture and technology are utterly enmeshed."*

- James Bridle (New Dark Age: Technology and the End of the Future, 2018)

## 1.3 RESEARCH METHODOLOGY

The framework that this thesis relies on is Value Sensitive Design (VSD) created by HCI scholars Batya Friedman and Peter Kahn in the 1990s (Friedman, 1997). To engage creators in accounting for human experience and values, VSD argues for the consideration of moral human values for the design of computer technology and that these should be involved as early as possible in the development process with a continued involvement throughout the project (Friedman, 1997). VSD is the inspiration behind the following hypothesis and research question:

### **Hypothesis:**

Embedding privacy values early on in the design and development process would help strengthen preventive approaches to privacy for smart workspaces.

### **Research Question:**

How might we integrate people-centered and place-centered privacy values in the design and development phase of creating smart workspaces?

There are two sub-questions to the broad research question: 1) what values must be considered, and 2) how might these be leveraged to create privacy-preserving interventions for smart buildings? In order to answer these, my approach was to first draw learnings from the perspective of occupants in an existing smart workspace, use these to generate people-centered and place-centered privacy values, and then put them across tangibly for creators. This essentially created a feedback loop between the influence of such interventions and the front end of the design and development phases.

**How might we integrate  
people-centered and place-centered privacy values  
in the design and development phase  
of creating smart workspaces?**

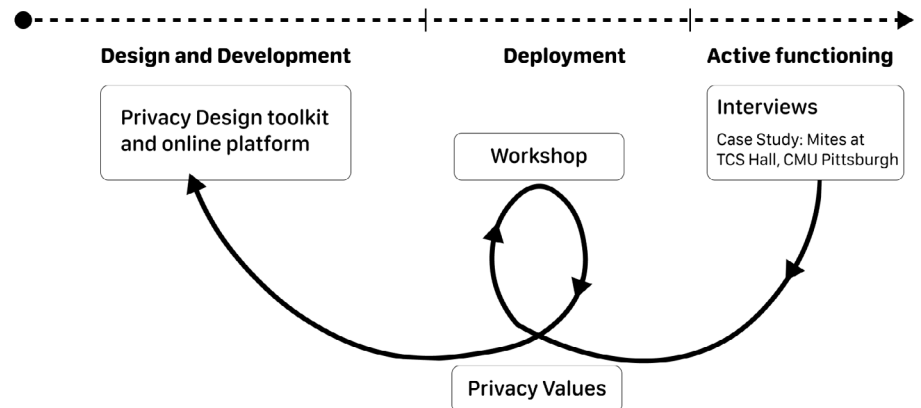


Fig 2. Research approach of creating a feedback loop

The existing smart workspace that I investigated for this thesis is TCS Hall at Carnegie Mellon University campus (described in section 5.2). Completed in 2021, this building is equipped with Mites, “a ubiquitous sensing platform” designed to create smart building applications and study user interaction with these (Mites FAQ document, p1). The building is used for work by students, researchers, faculty, administrative staff and visitors who occupy the common areas, hence it fits the definition of a smart workspace. I learned about the goals of the project through secondary research, and conducted primary research through silent observations of occupants’ behavior and seven 1-1 interviews that included a design probe. The insights from these interviews were crucial in having contextual learnings which also happens to be one of the proposed values.

## 1.4 INTENDED AUDIENCE

The target audience for this work is the creators behind smart workspace projects. This includes, but is not limited to, engineers, designers, technologists, architects, building managers and owners. Each of these diverse sets of professionals have a different focus while shaping such projects. For example, designers and architects focus on the occupants' experience, engineers focus on the technical details, and building managers focus on efficient functioning of the building. The final product is a cumulative outcome of the big and small decisions made by them, including the ones that impact privacy. Therefore, it is important to tie all these seemingly disparate decisions together to make privacy practices in smart buildings a preventive approach instead of a remedial one. Bearing this collective responsibility can be addressed by fostering an interdisciplinary dialogue among these professionals to think of data, people and place simultaneously for privacy.

Here, the term 'engineers' represents a broad category that includes IoT engineers, developers, privacy engineers and any other engineer who is closely engaged with designing the details for an IoT system for buildings. This group, in fact, is a key audience for this work to complement their heavy technical focus with a people and place-centered point of view.

## 1.5 SCOPE AND LIMITATIONS

- This thesis does not look at the aspects of data security and is only concerned with privacy practices.
- The proposed approach is meant to complement the existing approaches and not replace them. My hope is that these approaches would broaden the extent of current practices and expand opportunities to strengthen the 'Preventive not Remedial' approach to privacy (Cavoukian, 2009).
- It is important to emphasize that this study is qualitative and contextual for a shared space. Even though some concepts may be applicable to a different context like that of a smart home with some adaptation, the intent is neither to make any quantitative comparisons nor make claims about the domestic realm.
- The participants of primary research for this thesis were Privacy Engineers who work out of TCS Hall. They have more sound technical knowledge and exposure to privacy issues as compared to an average end-user or an occupant. This could raise concerns about their higher affinity toward privacy. However, with respect to TCS Hall and Mites, they are also the end-users or occupants subjected to ubiquitous sensing in their place of work without their will. This lends an interesting perspective to the study where the tensions and trade-offs between the benefits and risks of such technologies

adequately come to the fore.

- Due to time constraints, it was difficult to go deep into understanding a detailed process followed by each of the creator subcategories mentioned in 1.4. Conducted over a period of 8 months, this thesis lays the foundation for interdisciplinary approaches and would benefit from further work on integrating knowledge about the creators' processes.

## 1.6 AREAS OF INQUIRY AND THESIS OVERVIEW

In order to create novel privacy approaches for IoT-enabled physical spaces, it is important to understand privacy, from two different lenses.

- **Privacy, a computing lens:** In the last two decades, approaches for tackling data privacy on the internet have become more nuanced. The burgeoning trend of seeing buildings, and even whole cities, as computers means that the creators look to these approaches as they collect and process large amounts of data. An understanding of the current practices can serve as a useful basis to identify the gaps and create new approaches that complement them.
- **Privacy, a people-centric and place-centric lens:** Dr Alan Westin, who is regarded as the father of modern data privacy law stated that:

*"Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives"* (Westin, 1967, p.7)

This statement aptly captures the fact that privacy is deeply entangled with the relationships people hold with each other in a given context. In a non-domestic shared context like that of a smart workspace, individuals or groups seek varying optimal levels of social interactions at different times through a dynamic process of withdrawing and coming together. Privacy in these spaces is very much a socio-cultural phenomenon, and therefore, needs to be understood from the notion of the 'people' and 'place'. The word place here does not refer to just the physicality of a space but also how it is used, what are the associated social meanings, cultural notions, the relationships between occupants, appropriate behavior etc. (Dourish, 1996).

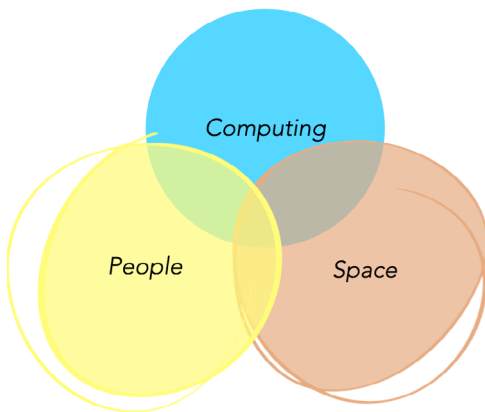


Fig 3. Framing privacy for smart buildings as an intersection of people, place and computing

The following 3 chapters establish the related work as per the following structure:

1. **Chapter 2 - 'Smartification' of the built environment:** to ground the framing of privacy for smart buildings as an intersection of people, place and computing.
2. **Chapter 3 - Understanding Privacy: from a computing lens** (a technological take) and a people-centric and place-centric lens (a socio-behavioral take).
3. **Chapter 4: 'Penumbra' of privacy for smart workspaces:** highlights the inadequacies of current approaches and the proposal for a new approach.

## 1.7 Key Definitions

### Privacy

For the purpose of this thesis, privacy is not equated with surveillance or the dystopian views associated with it. It is defined as follows:

- Privacy is a 'dialectic process', that involves a dynamic phenomenon of having control over what one wants to share with selected others and whatnot (Altman, 1975).
- "Privacy is not a solely "keep-out" or "let-in" process, it involves a synthesis of being in contact with others and being out of contact with others" (Altman, 1975) and is the opposite of a solely withdrawal process to avoid stimulus overload (Milgram 1970) or preventing intrusions (Schwartz 1968).
- Privacy does not equal secrecy but is an appropriate flow of information (Nissenbaum, 2009). Therefore, it involves understanding the harmony between the usefulness and harms of sharing information as well as the behaviors associated with it.
- In terms of digital and data privacy, it is not only about data collection (aka surveillance) but also about how the collected data may be used. Two key aspects to note under use are: 1) aggregation and inferencing (that is the practice of combining various pieces of data about an individual to conjecture who they are, where they are, what they like or do not like, what are they likely to buy or do etc.), and 2) disseminating that is sharing with others for a specific gain.

**People-centered**

People-centered is defined closely in alignment with human-centered wherein empathy for users drives the process. The reason for using the word people-centered is that it captures the messiness of human life better than the word human which reduces them to purely anatomical beings.

**Place-centered**

In the context of this thesis the word place 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. (Dourish, 1996). These meanings are what form memories, associations and communities and is an important definition to study privacy as it impacts the notion of control for individuals.

## CHAPTER 2.

# **'SMARTIFICATION' OF THE BUILT ENVIRONMENT**



**BUILDING INTERNET APPLIANCES**  
A TECHNICAL PERSPECTIVE

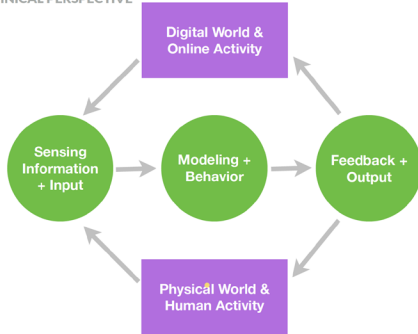


Figure 4: Diagram by Daragh Byrne, Designing for IoT course conducted at Carnegie Mellon University in Fall 2021.

The use of sensors in buildings is not a new concept. The earliest version of an electric thermostat was developed by Warren Johnson in July 1883 for his classroom (Brachmann, 2018). The impetus behind his invention was to reduce the hourly interruptions by the school janitor for checking the temperature on class thermometers to then adjust the amount of heating or cooling required. In the 1940s, Samuel Bagno created the first use case for motion sensing outside military applications to create an alarm system. The sensor detected the motion of a person by bouncing ultrasonic waves off inanimate objects in the room. Almost a century later, sensors in buildings today monitor a range of parameters: temperature, motion, humidity, air quality, water quality, proximity, brightness, color, sound, wifi strength etc. They may be embedded in objects or in the physical environment. Most importantly, they have become omnipresent and more sophisticated through their connectivity to the internet, commonly referred to as the Internet of Things or IoT. Internet connectivity enables these IoT devices to receive inputs from the physical world, transform them to data for collection and processing, and follow it up with an output action, either on the internet or in the physical world (McEwen, Cassimally, 2013). This makes IoT a giant network of things connected to human activity through data.

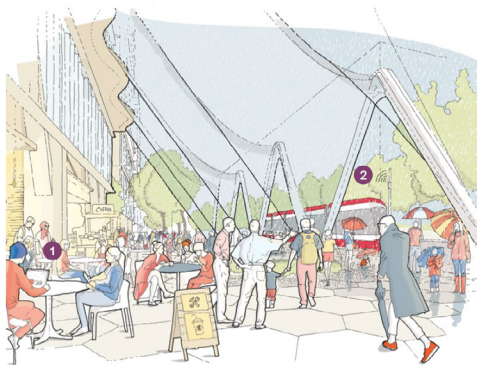


Figure 5: Rendering by Sidewalk Labs highlighting ubiquitous network as (1) and standardized physical mounts as (2)

The ability to use data for automated decision-making or an action is what gives IoT interventions the status of being 'smart'. For example, a smart fridge can monitor the expired contents in it and add them to the user's shopping list for the next grocery run. In the context of entire buildings, the ultimate goal of using smart solutions is to assist in efficient building operations and management. Some common examples include automated temperature control, giving selective access to occupants, energy conservation by automatically turning off lights when no one is in the space, identifying underutilized areas of shared spaces, detecting areas that need cleaning, and making elevators more efficient etc. These new capabilities have created a buzz of 'smart buildings' innovation in the past decade, whether they are residential spaces, retail environments, public spaces, or shared workspaces. There is a wave of transformation where the use of IoT is expected to slap on 'smartness' to existing buildings and cities, or even help create newer better versions from scratch. One recent example is Sidewalk Toronto by Sidewalk Labs which sought to create a smart neighborhood in the 'internet age' from the ground up until it shut down in mid-2020. The techno-solutionist vision of the project was rife with data privacy concerns, and if implemented, would have made the area "some of the most heavily surveilled real estate on the planet" (Sauter, 2018, para. 22).

It can not be denied that some of the smart building use cases may be useful. But the current buzz around them has led to a computation heavy narrative for the built environment. The hyperconnectivity of sensors, cameras, beacons, smartphones and operating systems connected via the internet, have created a problematic metaphor of the built environment as a 'computer' that can be programmed and neatly operationalized (Mattern, 2021). This is easily exemplified by a quick google search for the word 'smart buildings' which reveals cold, blue and gray images in which buildings and hardware transmit data without any sign of human life.

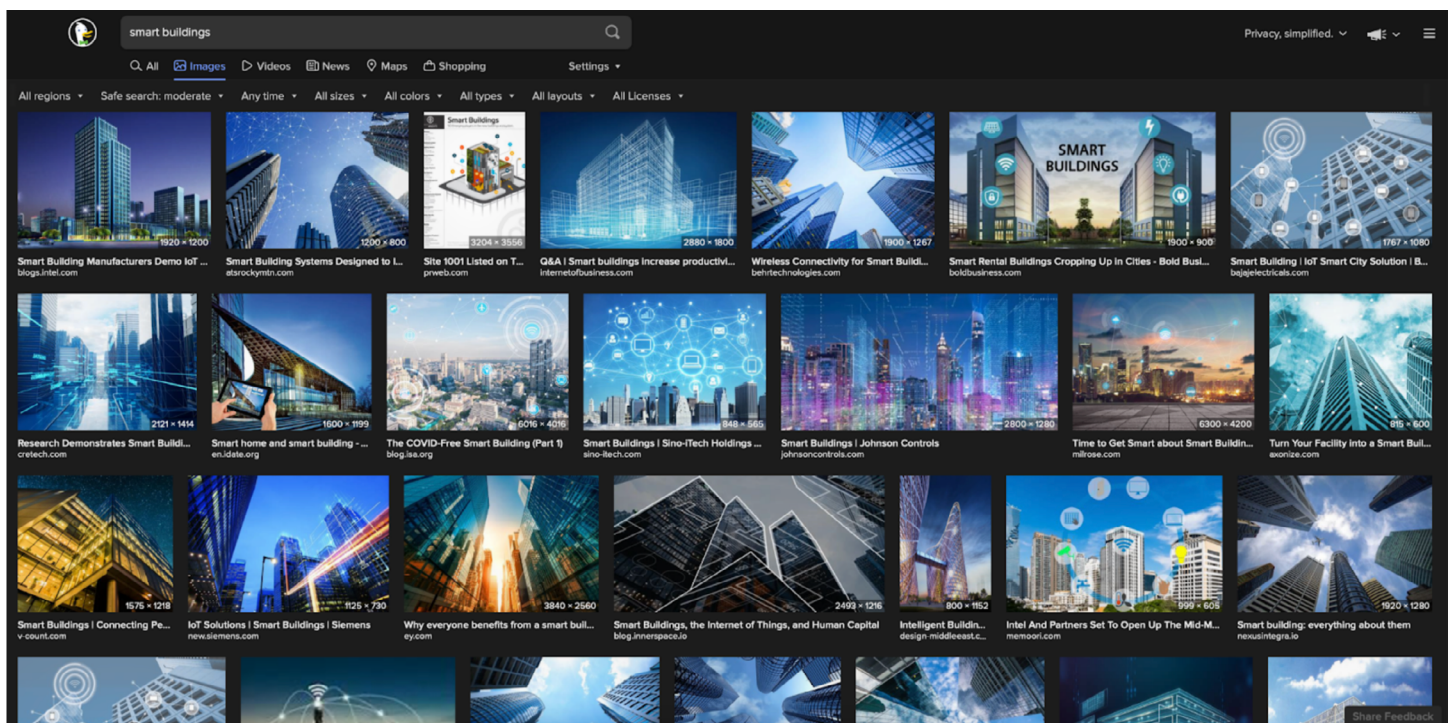


Figure 6: Screenshot of google image search results for the word 'smart buildings' which shows no sign of human life

Furthermore, echoing Mark Weiser's (1999) vision, a computer scientist and father of ubiquitous computing, smart building projects are obsessed with making the sensors invisible and seamlessly integrated in the physical environment. This computation first mold has suddenly reduced the built environment to a mere topic of engineering capabilities and managing infrastructure. Such goals are more concerned with the technological prowess and often ignore the discussion around the context for which it is being designed (Desjardins, 2019). These goals conceptualize smart buildings as an amalgamation of computing and architecture. The question then is, should smart buildings be seen as computers? And if so, should we conceptualize privacy for them from a purely computing lens?



Figure 7: Complementing technology with morals, values, ethics and humanity.

Source: [Technology vs Humanity: What will be our ethics, as we face "hellven". The Alternative UK](#)

In alignment with Shannon Mattern's point of view (Mattern, 2021), I argue that seeing buildings as computers is a flawed framing and lacks a human-centered perspective. A building, first and foremost, is a place where human life plays out. IoT in the context of smart buildings embodies the lived experiences of the people in these places 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 about human activities in physical spaces is, thus, a narrative of the human experience, behavior, values and ways of being in that context. Hence, the digital aspects of making buildings smart cannot be seen in isolation from the aspects of human life. By extension, data and privacy in smart buildings cannot be seen in isolation from the people and place with which it is bound. Therefore, I offer two re-framings to investigate at privacy in the context of smart workspaces

1. Conceptualizing data and privacy from a people-centric, place-centric and a computing lens simultaneously (described in chapter 3). This is because data collected by IoT are never going to be place agnostic or devoid of meanings of its context (Loukissas, 2019) and therefore neither can privacy be. Many scholars have argued that data is not independent of the setting in which it is collected and beyond the mere numbers, it represents the qualitative aspects of these settings. Some of these scholars include anthropologists like Genevieve Bell and Tricia Wang, Yanni A. Loukissas, an author and Associate Professor of Digital Media at Georgia Institute of Technology, data feminists like Catherine D'Ignazio & Lauren Klein, Information Designers like Giorgia Lupi, and interaction design researcher and Educator like Audrey Desjardins. To illustrate a simple example, peers may stay in the workspace till after hours to work flexibly at their own pace or to hang out if it is an acceptable behavior in the organization. This granularity of acceptable behavioral norms cannot be portrayed by data in a strictly algorithmic sense, thereby creating the need to complement a computing focussed perspective with a socio-behavioral one.
2. Create preventive instead of remedial approaches by embedding people-centric and place-centric privacy values in the front end of the design process for creating smart workspaces. This is inspired by two of the seven Privacy by Design principles proposed by Dr Ann. Cavoikian: i) proactive not reactive, preventative not remedial, ii) privacy embedded into design (Cavoukian, 2009). The two key differences between these principles and my reframing is the focus on the design process for the creators, not just the final outcome and the use of a values-based approach to achieve this. I discuss these differences in chapters 4 and 5.

## CHAPTER 3.

# **UNDERSTANDING PRIVACY**

Dr. Alan Westin, who is regarded as the father of modern data privacy law, recognized that "...dealing with the issue of data privacy would require a mix of legal, social and technological solutions" (Fox quoting Rosen, 2013). Concurrent with this argument, this thesis looks at privacy from two lenses: a computing lens to understand the status quo of current data privacy practices, and a people-centric and place-centric lens to understand privacy as a socio-cultural and behavioral phenomenon. The understanding of the former would help to look at privacy from a legal and technological purview and the latter would help understand it from a human-centered point of view. Together, they would help to draw connections between people, place and computing aspects of privacy.

### **3.1 A COMPUTING LENS, OR THE 'UMBRA' OF DIGITAL PRIVACY**

When the internet was first commercialized in the eighties, the privacy of its users and what they do were not a primary consideration. In today's context, it has become a place to hoard user data in exchange for the use of digital services. There is an inherent tradeoff between their value proposition and the privacy of the individuals whose data is collected, aggregated, inferred and disseminated. This tradeoff is often tipped in the favor of extensive amounts of data collection and inferencing, thereby exacerbating privacy concerns. The data privacy problem has garnered attention in the last two decades by technologists, scholars and regulators leading to tactics for repairing privacy on the internet. The current tactics can be divided into 3 categories that revolve around: i) bringing transparency to existing practices (through usability, better notices etc.), ii) data management (through policy, regulation, organizational strategy or technological solutions), iii) creating stand-alone technological solutions to empower end-users to protect themselves from existing undesirable practices (also called Privacy-enhancing technologies or PETs). Collectively, these three categories have set the status quo for most other technologies to follow, thereby forming the 'umbra' of privacy approaches in the digital era. It is important to note that these are all different from data protection, aka security, which is out of the scope of this thesis.

#### **Transparency for existing practices**

The first and the most popular tactic for this is notice and consent. The notice and consent is an industry 'self-regulated' mechanism that is part of the Fair Information Practice Principles (or FIPPs) from 1973. It seeks to give users information about data collection and use practices of the organization through a 'meaningful Notice', along with the ability to consent to them. The core component of notice is laying out either the entire privacy policy



or aspects of it in a manner that catches user attention. This may be done by 'posting an information practice disclosure on the web' (as mentioned by the Federal Trade Commission) or through a pop-up notification (as in the case of most websites that ask users to accept or reject 'cookies') or through a physical notice in case of technologies that collect data in physical environments. Whatever the mechanism, the practice of notice and consent is a principle and not a legal framework in most cases, except General Data Protection Regulation (GDPR) and the California Privacy Act (CCPA).

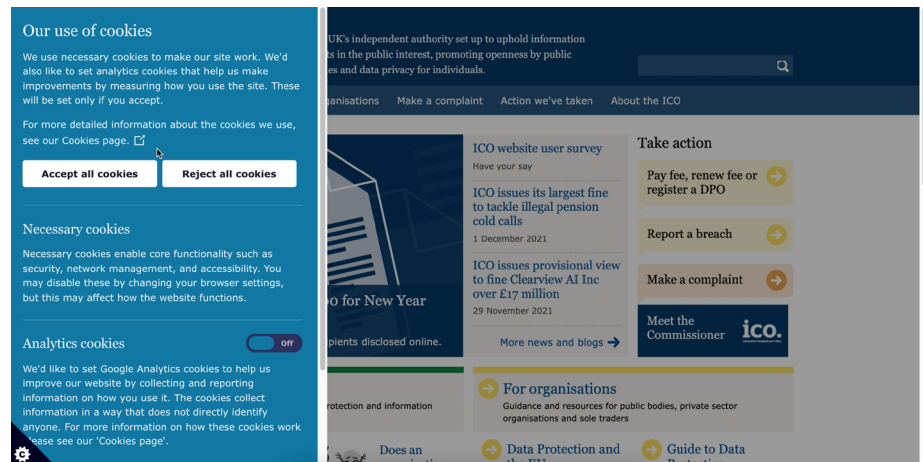


Figure 8: Screenshot of a Notice and Consent example for cookies

There has been considerable criticism for this principle in practice as it entitles the organizations to any form of data collection and use (Solove, 2013). From a user perspective, it is certainly not enough as it does not give them any real agency over their data. They are expected to check a box based on reading a short message, if at all they do, and make privacy tradeoffs, advertently or inadvertently. Additionally, given the number of digital interactions today, it is virtually impossible that users can pay attention to the nuances of privacy policies conveyed in any form (McDonald and Cranor, 2008).

Another practice that aids in bringing transparency from a user-centric perspective is usable privacy and security. It is built on the foundation that abiding by guidelines or meeting regulatory requirements doesn't necessarily mean that users can easily find, understand or successfully control their privacy preferences (Schaub and Cranor, 2020). Hence, usable privacy and security is the use of human-computer interaction design techniques to create usable and useful privacy interfaces for users (Cranor, Garfinkel, 2005). An interesting example of a useful interface design element is the privacy "nutrition" label for IoT devices developed by the CUPS lab at Carnegie



Figure 9: Privacy nutrition created for IoT devices developed by the CUPS lab at Carnegie Mellon University

Mellon University. Much like the FDA nutritional labels that give consumers the information about food ingredients, the privacy labels for IoT devices give users transparency in how organizations are collecting, using, and sharing their personal information (Kelley, Bresee, Cranor, Reeder, SOUPS, 2009). These have had a slow adoption in the industry but may have inspired the creation of Apple's privacy nutrition labels.

## Data management

This includes making decisions around data practices, creation of privacy policy, responding to user concerns and ensuring compliance with both company policies and legal frameworks. These responsibilities are often cemented in the role of a Chief Privacy Officer who is the central point of contact for privacy issues. In terms of making decisions for data practices, these may be statistical approaches for dealing with datasets like differential privacy or strategic ones like de-identification or de-anonymization of personal data once it is collected. De-identification is the process of removing some identifiers about an individual (like location, zipcode, age, sex, date of birth etc.) in a manner that the data remains useful without revealing the identity of any individual. However, this has proven to be insufficient in practice. When a number of identifiers about an individual can be triangulated either from different datasets or over a period of time, it can coherently point to an individual.

## Empowering users through PETs

Privacy-enhancing technologies (PETs) are technological solutions specially designed to circumvent privacy vulnerabilities for users. They do so by minimizing the collection of their personal data while still allowing the functionality of the digital system or service being used. Some common examples include ad block plugins that prevent tracking and targeting for ads, password managers that store user passwords securely in one place and duck duck go browser that does not store search history or personal data and therefore does not sell it to third parties. Privacy tech is a growing field and the coming together of decades worth of privacy research, the increased attention by regulatory bodies, increased awareness of users and most recently, venture capitalists' interest in investing in privacy solutions. However, two key shortcomings of PETs are that they are not widely known to average users and that they require a little extra effort on the part of the user. These factors depend on user awareness and motivation thereby limiting their impact to those who are aware and motivated to go the extra mile to protect their privacy.

### 3.2 A PEOPLE-CENTRIC AND PLACE-CENTRIC LENS

The concept of privacy has existed for humankind for centuries. It appears in several disciplines: anthropology, psychology, sociology, law and architecture, and therefore has been studied by scholars from multiple different perspectives. In 1967, Alan Westin, a Professor of Public Law & Government Emeritus, Columbia University, weaved together different facets of privacy from a myriad of disciplines in his book 'Privacy and Freedom'. Although the book was written in the context of growing popularity of computing and electronic records in 1960s, it made two important contributions:

1. It provided the first systematic analysis of privacy as the ability to control how much one reveals about themselves to others. This definition has formed a useful basis for much of the privacy discourse in all disciplines that have entanglements with the subject, including social science and laws governing digital privacy.
2. Building on the idea of control over the extent and flow of information, Westin also conceptualized 4 states of privacy: Solitude, Intimacy, Anonymity, and Reserve.



**Solitude:** an individual alone and free from observation of others.



**Intimacy:** an individual is part of a small unit and exercises seclusion from those outside it.



**Anonymity:** an individual in public but still seeks and finds freedom from personal identification, as if "lost in crowd" (Altman, 1975).



**Reserve:** an individual creates a psychological barrier against unwanted intrusion by limiting information flow

From a behavioral point of view, these categories highlight the idea of an individual's openness or closeness to sharing with respect to interactions in different sizes of social units. These interactions also have an element of environmental factors that may enable, disable or necessitate seeking such states. The role of environmental factors, in particular, has been elaborated by other scholars who noted that one of the important factors for exercising freedom of choice, and hence privacy, is the control over space (Proshansky, Ittelson and Rivlin, 1970). The control over space often manifests in the form of territoriality thereby increasing the range of behavioral options available to an individual. When seen holistically, what comes to the fore is the deep relationship between the social and environmental conditions that shape privacy behaviors. This interdependence of the two is best highlighted by Irwin Altman (Altman, 1975), a social psychologist whose work on privacy fits well with this thesis and is defined here.



Altman defined privacy as a dialectic process of withdrawing and coming together, as opposed to a sole withdrawal process to avoid stimulus overload, as postulated by Milgram in 1970, or preventing intrusions as noted by Schwartz in 1968 (Altman, 1975). This distinction is important, especially because in a non-domestic context like that of a smart workspace, the interactions between people vary on a spectrum of person to person and group to group, and every combination in between. In such contexts, individuals or groups seek varying optimal levels of social interactions at different times, but the dynamic process of withdrawing and coming together may be unavoidable, or necessary or sometimes even desirable. An individual or group's desire to achieve an optimal level of privacy is then expressed through four different behaviors: verbal, non-verbal, environmental behaviors and cultural norms (Altman, 1975).

### **Verbal Behavior**

Explicit instruction through the use of spoken language. For example "Leave me alone".

### **Non-verbal use of the body**

Also known as body language. For example, turning away when an unwanted immediacy of a stranger is encountered. Today this also applies to how individuals in public spaces may sit with their back to the walls so that their laptop is not visible to anyone else or wearing headphones to disconnect from the immediate environment while still being physically present.

### **Environmental behaviors**

Setting boundaries and regulating the permeability through these. There are two elements to these, first is that of personal space which is a boundary surrounding the self. This may be an invisible zone expressed during interactions, like comfortable proximity while talking to a stranger v/s a close friend, or a visible boundary demarcating access to physical space, like access to one's own room or avoiding intrusion from neighbors. The second is the territory, that is regulating access to space through markers, areas, and objects. These territories can be central to an individual or groups' life and have long-term control such as bedrooms or homes, or can be public in nature with temporary and/or limited access such as occupying a table at a restaurant or claiming a go-to neighborhood bar. An intrusion into any of these boundaries causes a violation of privacy for the occupant and leads to verbal, non-verbal or active defense.

### **Culturally defined norms and practices**

The notion of privacy exists in all cultures and societies but carries different meanings, and therefore different behaviors, for creating a separation between the self and others. For example, in most Western cultures, physical barriers and related gestures to cross them are crucial for ensuring Privacy, whereas in Polynesian societies individuals often have little physical privacy and sleep side by side (Lee D. cited by Westin), in what might be considered a 'crowded condition' by most Westerners. Altman also highlights the example of Javanese society studied by the anthropologist Clifford Geertz, where privacy is achieved not by environmental barriers but by psychological techniques like not expressing feelings easily to maintain an interpersonal reserve. From my own experience as an Indian, the idea of drawing boundaries with family members carries a different notion and is expressed differently as compared to the notions in Western culture. A plethora of relevant examples and behaviors across the world highlight that while the need for privacy may be universal, the practices and nuances make it a culturally situated phenomenon.

CHAPTER 4.

**CREATING 'PENUMBRA' OF PRIVACY  
FOR SMART WORKSPACES**

The existing practices that address digital privacy have become more nuanced over the years and have made substantial contributions. However, since most of these approaches evolved as a reactionary response to growing privacy concerns on the internet, they still do not move the needle for making privacy a forethought than an afterthought. For example, most of the FIPPs principles, including notice and consent, have been reduced to narrow, regulatory requirements that satisfy a checkbox. These principles do not give any real agency to the people whose data are collected and processed, and reflect a procedural approach to maximizing control by xxx rather than individual or societal welfare (Cate, 2006). Approaches like de-identification that prevent revealing the identity of an individual seem ideal but fail in practice when data from a large number of datasets is aggregated. PETs, on the other hand, are effective but are not widely known and sometimes require additional effort on the part of the users. All these disjointed efforts at different scales ranging from policy and regulation, to organizational strategy, and to empowering individuals with digital tools have created change, but are still inadequate for two key reasons:

1. They try to fix privacy after the fact, without asking critical questions about the reasons, the impact, the ethics and morals behind the data practices; thereby making them remedial approaches.
2. They fail to adequately integrate the socio-behavioral perspectives for privacy, highlighting the age-old disconnect between CS (computer science) and STS (Science, Technology, and Society) perspectives.

The inadequacy of the current practices makes them unfit for their direct transference to emerging technology including IoT applications for buildings (Greenfield, 2006). Despite proving insufficient, they have set the status quo, or 'umbra', for conceptualizing privacy for smart buildings. For such projects, the two in particular that are used as an argument for bagging the 'privacy-preserving' tag are notice and consent, and de-identification of personal information. The trend of smart buildings is catching on globally but is in relatively nascent stages of its development. Right now is the ideal opportunity to make these innovations privacy-preserving from the get-go. To do so, it is important to go beyond the status quo of the current practices and create broader approaches, or penumbras, that are human-centered. The two insufficiencies stated above can be addressed by creating i) a preventative approach rather than remedial, and ii) an approach that accounts for the socio-cultural norms, behaviors and fundamental human values. The latter is equally important because the nature of interactions and relationships between people in shared physical spaces is very much a socio-cultural phenomenon, and hence impacts the very notion of privacy (section 3.2).

When IoT applications ignore this and only think about data and algorithms, they lack the granularity to portray the qualitative aspects of human life. Therefore to undertake i) and ii) simultaneously, I propose an approach based on human values to be plugged in at the front end of the innovation process of creators. More specifically, the idea is to embed people-centric and place-centric privacy values in the design and development phase of creating smart workspaces and positively influence it from the get-go. Such an approach is meant to complement the current approaches and hopefully also strengthen them. When IoT applications ignore this and only think about data and algorithms, they lack the granularity to portray the qualitative aspects of human-life. Therefore to undertake i) and ii) simultaneously, I propose an approach based on human values to be plugged in at the front end of the innovation process of creators. More specifically, the idea is to embed people-centric and place-centric privacy values in the design and development phase of creation of smart workspaces and positively influence it from the get-go. Such an approach is meant to complement the current approaches and hopefully also strengthen them.

The proposed theory is inspired by two existing bodies of work: Privacy by Design (PbD) principles developed by Dr. Ann Cavoukian (Cavoukian, 2009) and Value Sensitive Design (VSD) framework created by HCI scholars Batya Friedman and Peter Kahn in the 1990s (Friedman, 1997). The two PbD principles that align well with this thesis are: i) proactive not reactive, preventative not remedial, ii) privacy embedded into design (Cavoukian, 2009). These principles have been criticized as vague and difficult to apply in practice. This insight was confirmed when I asked around 15 privacy professionals during a data privacy workshop at CSCW 2021 as to whether they used these principles. The responses to my question highlighted that not only are these principles difficult to apply in practice, but there are no incentives to think of privacy by design currently. To make preventative practices more tangible and approachable, my proposal focuses on the design process for the creators, not just the final outcome as in the case of PbD and leverages a values-based approach in alignment with VSD. VSD seeks to design technology with ethical import by integrating moral human values using conceptual and empirical investigations and is described in the following chapter.

*PART II: TOOLKIT DEVELOPMENT*

CHAPTER 5.  
**RESEARCH METHODOLOGY**

## 5.1 VALUES BASED APPROACH

Value Sensitive Design framework (VSD) argues for the integration of moral human values in the process of creating technology (Friedman, 1997). Drawing a clear distinction between personal values (of an individual), moral values (based on human welfare) and conventional values (for social interactions), it postulates the need to embed moral human values in the design of technology. The framework has three components: conceptual investigation, done through literature review, empirical investigation, done through primary research and technical investigation that is designing the technical details of a computing system. It is important to note that as per VSD, human values should be engaged early on, and throughout the process. This has been a key inspiration for my hypothesis and research question:

### Hypothesis:

Embedding privacy values early on in the design and development process would help strengthen preventive approaches to privacy for smart workspaces.

### Research Question:

How might we integrate people-centered and place-centered privacy values in the design and development phase of creating smart workspaces?

There are two sub questions to the broad research question: what values must be considered and how might these be leveraged to create privacy-preserving interventions for smart buildings? In order to answer these, my approach was to first draw learnings from the perspective of occupants in an existing smart workspace to then put them across tangibly for creators. This also created a feedback loop between the occupants and the decision-makers for IoT. This was achieved by:

1. Engaging the Occupants to generate values: A functioning smart workspace on Carnegie Mellon University campus was investigated to generate relevant privacy values (section 6.1 - 6.3). The reason behind this was that values are context-dependent and rooted in the nature of human relationships in that context and I wanted the ability to interact and make observations in person. For example, values for a smart home would be different from a workspace which would be different from a retail space. Therefore, it was important to not make assumptions or introduce bias in what values are relevant.
2. Integrating Values in practice for creators: The values identified for a smart workspace context were made tangible and approachable, and integrated as a part of a toolkit (section 6.6 - 6.6, 7.1).

How might we integrate  
people-centered and place-centered privacy values  
in the design and development phase  
of creating smart workspaces?

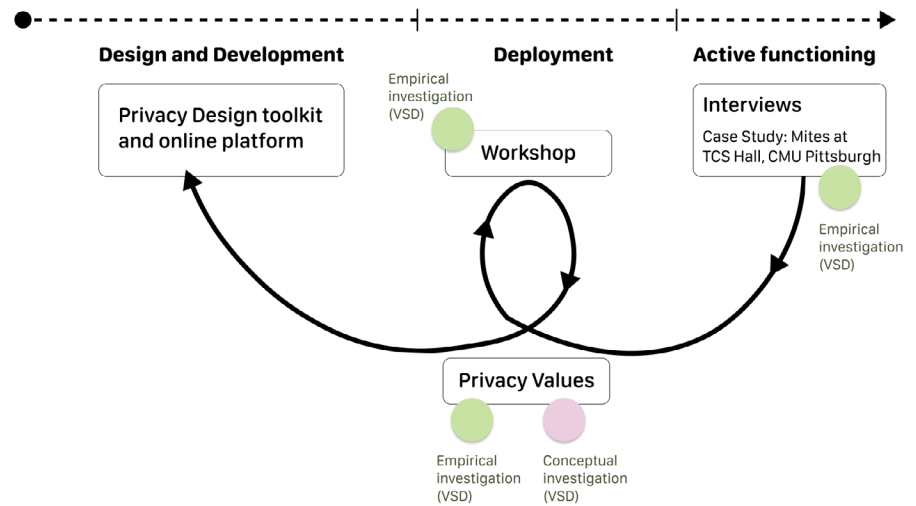


Fig 10. Research methodology of creating a feedback loop through conceptual and empirical investigation

The following table represents the two sub-questions with the respective design and research activities:

| Sub-question  | Research and Design 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?"           | <ol style="list-style-type: none"> <li>1. Conduct interviews</li> <li>2. Synthesize insights</li> <li>3. Generate people-centered and place-centered values</li> </ol>   |
| "How might we leverage different privacy values to facilitate the creation of privacy-preserving interventions for smart buildings by interdisciplinary teams?" | <ol style="list-style-type: none"> <li>4. Preliminary test of values through a workshop</li> <li>5. Make values more tangible and approachable</li> <li>6. Create Privacy toolkit for smart buildings</li> </ol> |

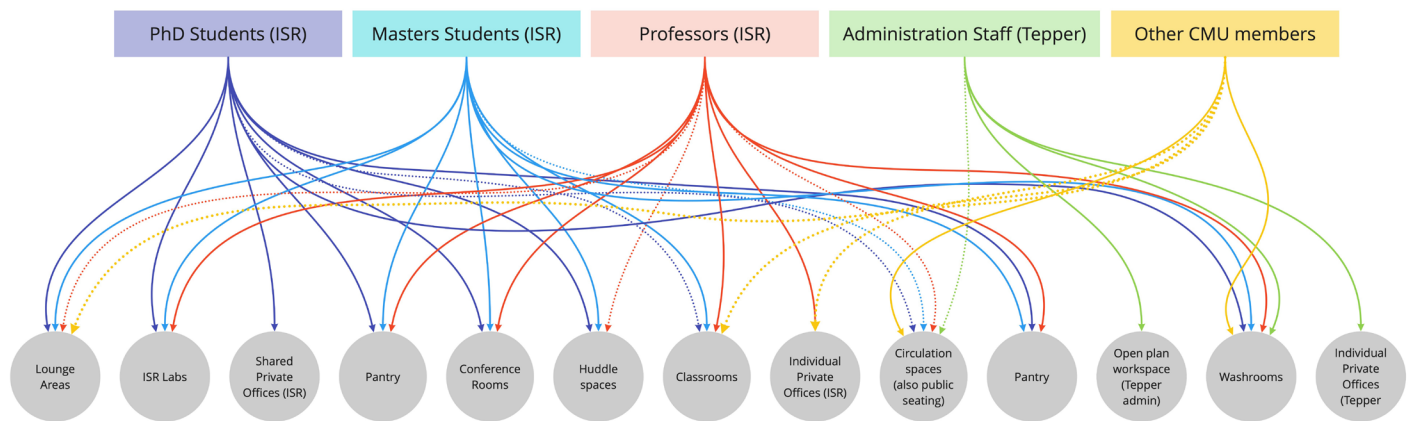
The existing smart workspace that I investigated for this thesis is TCS Hall at Carnegie Mellon University campus. I started by making silent observations in the building, followed by seven one-on-one interviews with occupants. This case study is described in the next section.



## 5.2 CASE STUDY

Mites is an “ultra-robust a ubiquitous sensing platform” (Miest FAQ document p.1) at TCS Hall at Carnegie Mellon University campus. It can be considered a co-working space as its occupants include a variety of groups for the purpose of work: 1) Permanent occupants including students and professors from the Institute for Software Research (ISR); and individuals who work for Tepper Administration, 2) Visitors to the building. The visitors are CMU members who have access to the public areas of the building through their university access card and use the seating in the publicly accessible parts of the building. Given the mix of stakeholders who use the building, the key assumption is that privacy decisions in such contexts are collective decisions rather than purely individual preferences.

Fig 11. Occupants of TCS Hall and the spaces they use



The website for the project defines the scope broadly as ‘future applications’ for Smart Buildings, which I argue to be a ‘techno-solutionist’ perspective. This makes the project an interesting case study for my research for three reasons:

### Insufficient Notice

It argues to have considered a privacy-first perspective in its design, by ensuring de-identification of individual data and through a notice as a letter-sized printout posted at multiple locations within the building (fig 12). From the first look, the notice does not give substantial or useful information about the nuances of privacy, as it merely lists the 12 sensors without clarifying the nuances of how the collected data would be used and disseminated, who has access to it, what choices do occupants have etc. The QR in the notice leads to the 20-page FAQ document that includes questions about how the data will be collected, and secured and how selected groups of occupants might be able to opt-out by writing an email to the researchers. The absolute lack of questions about ‘Why’ this is being done repeats the narrative of collecting large amounts of data without a clear intent. This perpetuates a tech for tech

sake perspective. The insufficiency of this notice was also confirmed by the participants in the interviews, yet this is used as the first argument of a privacy-preserving perspective.

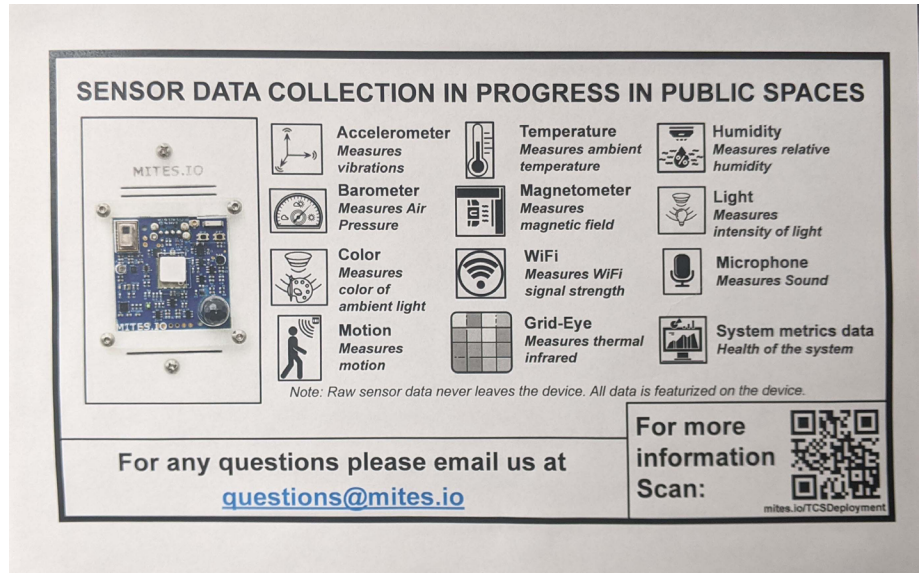


Fig 12. Mites notice that includes a QR code to a 20-page FAQ document

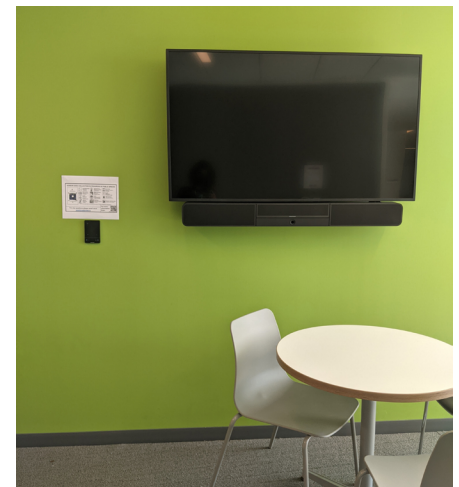


Fig 13. Mites notice in different spaces

## Occupants as intended audience

The occupants of this building include students of the Master's Privacy engineering program who are future privacy experts, but are simultaneously the occupants implicated by this technology without a say. They work, laugh, rest, share and sometimes even dance in this space celebration of finishing an assignment. This irony, and the question of what ideas does this sort of a project normalize for them, makes them an interesting group for conducting this research. Additionally, they are a subset of the creators that may be involved in smart workspace projects in the future.

## Techno-solutionism

It follows the approach of collecting large amounts of data without any deliberation on the intention and subsequently, the privacy concerns it may lead to. Similar to how things have unfolded for privacy on the internet, Mites in its current form fails to exemplify a balanced approach between the benefits of IoT for buildings and the associated privacy risks, both in the present and for the future. This is important because the research of this nature at prestigious universities like CMU sets a precedent for similar interventions to follow, hence it carries a hefty responsibility.

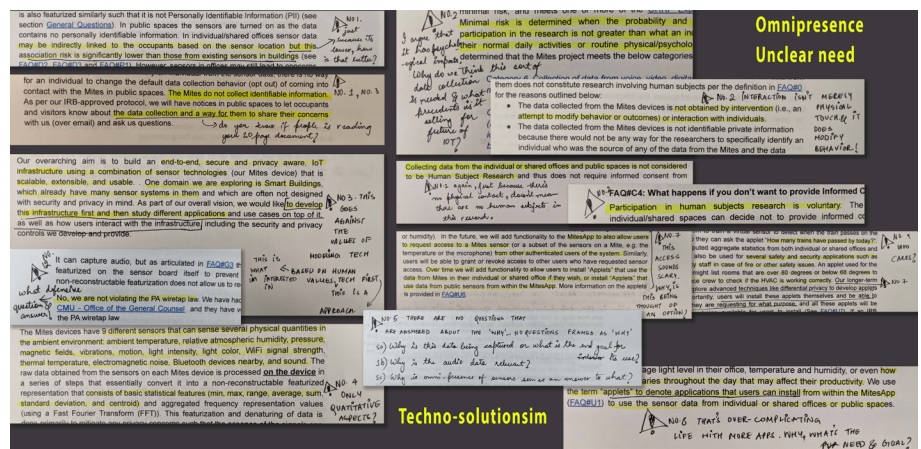


Fig 14. My notes on nuances of Mites

Because this technology is neither fully developed nor well thought through in its design yet, it's great this conversation is being had now instead of after the fact. In advocating for the people/humans in spaces who would be implicated by technology of this nature, I'm using this as an exemplar to explore alternate ways of thinking about privacy in the context of IoT-enabled physical spaces where so much of human life plays out.

## CHAPTER 6.

# **EXPLORATION, GENERATION AND ITERATION**

## 6.1 INTERVIEWS

The 1:1 interviews were conducted on Zoom and designed to have two components: conversation and a design probe on Miro. The decision to conduct interviews on Zoom enabled the participants to participate more flexibly while ensuring easy documentation for me through Miro. Additionally, I paid careful attention to the experience of the participants going through the interview and created smooth transitions between each part. The structure of the interview was as follows:

**General Privacy Mental Model and Perceptions:** This section included open-ended questions to understand the participant's general notions of privacy based on their experience and their everyday life. For example, one of the questions was 'How do you protect your privacy when you are around a roommate, your partner or a family member?' This consumed the first 10 minutes of the interview, but was a conscious choice to shake the software focussed mindset of my participants before diving deeper and for them to be more reflective during the process.


**Privacy for IoT and Mites:** This section organically carried over the conversation from the previous section through the question 'How do you protect your privacy in your current workspace at TCS?'. This was followed up with questions about Mites and the respective notice in the building, which were framed with a neutral tone assuming that they may not have prior knowledge of the project. Given this assumption, the participants were shown images of both the sensors and the notice on Miro which also facilitated a smooth transition to the design probe on Miro.

**Design Probe:** Seven Miro boards were set up with the same design probe, one for each participant along with a unique password. The interviewees were sent the link to their board and the password during the interview, and no interviewee had access to another participant's board. After they successfully joined the board, they were given a quick overview of how to write on a sticky note and how to move a sticky note followed by three activities.


1. Step 1- Rose Thorn Bud: Listing the Benefits (Rose), Privacy Risks/Harms (Thorn) and potential opportunities (Bud) for Mites on color-coded stickies.
2. Step 2 - Privacy-preserving actions: Talking through the actions they take to mitigate or avoid some of the privacy risks they wrote.

1.1: Rose, Thorn, Bud

**As of Today**  
 Context: Current deployment in TCS building  
Note: The number of stickies in each section don't have to be equal.  
Write as little or as much in each category that you feel is necessary.

**Rose**  
  
 What are the **Benefits** provided by the IoT sensors?

better analysis of how the building is used

**Thorn**  
  
 What are the **Privacy Risks/Harms** of the IoT sensors?

extra level of surveillance that is not inherent in the purpose of the space

people may not feel comfortable in the space because of increased level of surveillance

it may lead to increased security measures which may be uncomfortable for the space


people may face consequences for certain uses of the space which may not have been identified before

lack of collection/use limitation

set a new precedence for surveillance on campus

could be used to make the space more accessible

could introduce new efficiencies in energy expenditure depending on what decisions this data will be used to affect

**Bud**  
  
 What **Potential new Opportunities** might be created through the use of IoT sensors?

could be used to make the space more accessible

could introduce new efficiencies in energy expenditure depending on what decisions this data will be used to affect

Figure 15: Rose, Thorn, Bud activity as a part of design probe

3. Step 3 - Prioritization and Walk-through: Placing the Rose Bud and Thorn stickies on a spectrum from 'Most Important to Consider' to 'Least Important to Consider'. The choice of a spectrum over a Likert scale was a strategic decision to help participants think of the benefits, privacy risks and opportunities with respect to each other instead of in absolute terms. This is because these three categories have complex entanglements and specific things they wrote in each category may conflict with the others, yet they coexist and lead to trade-offs. Therefore they were instructed to interpret the in-between flexibly instead of 5-point or 7-point scales and talk through their thought process as they moved the stickies from each category. They were allowed to make changes until they felt that the relative placement of everything painted a holistic picture of Mites from their perspective.

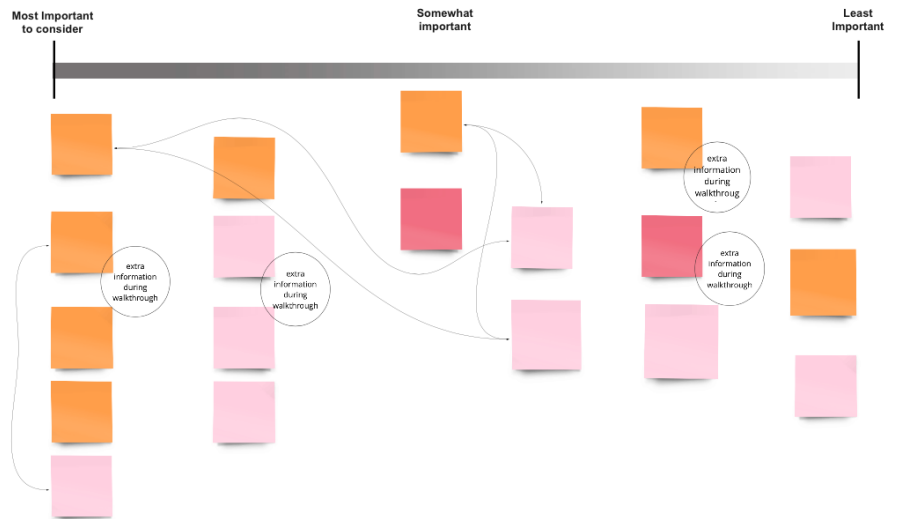


Figure 16: Example of prioritization for trade-offs, data has been removed for the purpose of privacy

4. **Step 4 - Trade-offs and Discussion:** As a wrap-up, the participants were asked to reflect on their prioritization holistically and identify direct or indirect conflicts/ trade-offs between the benefits, risks and opportunities. The interview ended by giving them the opportunity to share anything else that they would like but did not get a chance to.

**Note:** Barring any technical difficulties or participants' expression of difficulty in working with Miro for any reason, the participants were expected to write and move stickies on their own so that their flow of thinking was more natural.



## 6.2 INTERVIEW INSIGHTS

All interviews were recorded on Zoom and the transcripts were analyzed using Affinity Mapping on Miro. The following themes emerged through this mapping:

### **Fear of Normalization of Surveillance**

The concern around normalization of surveillance came up in most conversations but there was no consistency between how much weight participants put on it through the placement on the prioritization spectrum. In some cases, there was an observable undertone of concern that seeing sensors everywhere is numbing people towards their presence leading to individuals giving up on their privacy, both at TCS and elsewhere. Additionally, one participant framed it as a larger concern around the precedents for technology being set through a project of this nature.

*"Sometimes you see something so much it just becomes part of the furniture in a way."*

Participant RotM7w

### **Lack of Clarity on Purpose, Benefits and Data Practices**

On a high level, all participants understood that Mites sensors aim to aid efficient and effective building management, yet neither of them knew what exactly that meant and how it impacted them. They were aware of the presence of letter-sized notices in this regard, yet only 1 out of 7 had paid careful attention to it and scanned the QR code "out of curiosity and concern." As for the content of the notice itself, 7 out of 7 participants expressed that the notice did not give them any useful information about:

1. The actual use cases that justified the collection of this data,
2. The data practices like: what is each data type going to be used for, are multiple data points going to be combined for behavioral analysis, what all can be inferred, how long would the data be stored etc.,
3. Who is accountable for compliance with ethical data practices,

The choices for occupants to opt-out.

This highlights that creating an effective and useful notice is an important task in a project of this nature but beyond the scope of this thesis.



At the end of each interview, I opened up the conversation for the participants, that if they wanted to, they were welcome to touch on anything relevant that we didn't have a chance to talk about. Most of the time, they used this as an opportunity to ask if I had more knowledge of the project than they did. Understandably, the lack of clarity on the exact purpose of the project, how it benefits them and others in the building as well as the associated risks caused apprehensions and fears. This coupled with the fact that they can anticipate risks more easily as privacy engineers, made them feel all the more curious.

### **Contextual gestures to attain privacy**

Based on questions about how people attain privacy at TCS as well as in general, some themes emerged in alignment with Irwin Altman's conceptualization of privacy mechanisms.

#### **Verbal Behavior**

- Speaking at a lower volume while taking a personal call.
- Asking for callbacks at another time to be careful about what information they share while at TCS.

#### **Non-verbal use of the body**

- Sitting next to a wall or a window so that the laptop isn't visible to anyone else.
- Wearing headphones, especially while listening to something for which they fear they'll be judged by their peers or so that no one asks questions in case they receive a lot of text messages.
- Not drawing attention to themselves by bending in.
- Limiting the number of people they see or interact with.

**Environmental behavior:** Leveraging a physical barrier like closing the door or drawing the blinds

### **Finding anonymity in crowd and public spaces**

The deep relationship between space and privacy was highlighted in the interviews when most of the participants mentioned how they try to draw clear boundaries between parts of their life while they are at TCS. Most of them prefer to not talk about family-related or other sensitive topics in the relatively private areas like the classroom. They go to more public areas to take such calls, for example, corners or tables in corridors or walk around the hallway or all the way out onto the street. The motivation sometimes is to get away from the microphones, but most often it is a tactic to ensure that no one they work closely with hears those conversations. One recalled a similar past experience and overtly referred to this tendency of seeking 'anonymity in the crowd' in alignment with Westin's states of privacy:

*"...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 Forbes avenue during the workday than at TCS."*

Participant 8ZwXia

### **Feeling of Helplessness**

My selected audience: Privacy engineering students are in some ways temporary occupants of the TCS building. The key discussions around Mites, or any similar intervention, often do not engage a fleeting group of stakeholders like this one that is expected to be around for a rather short period of time (one and a half years in this case). As a result, the students feel like they have less say in what they are subjected to. Hence, despite their discomfort, they would rather focus on their priorities at school than spend time worrying about Mites. A participant mentioned:

*"...it's like it adds a cost to being in this building that I would rather not be there, especially for like a building with the purpose of what TCS is for, which is studying and working...unfortunately I have to use TCS for a lot of stuff so I just kind of have to like get over it, I guess."*

Participant HSqzq3

*"Maybe it's inevitable that I live with this thing for this year, but if I use this space and work my ass off in the space, then maybe one day i'll be working for a congressperson who passes a law that makes these technologies everywhere respect people better."*

Participant kDiWCB

### **The Conflict between Trust and Discomfort**

Almost all participants had mixed feelings about Mites as a research project. While they felt uncomfortable being surrounded by these sensors, especially given the unclear nature of the entire project, they also placed a certain level of trust in it. The degree of trust varied, but the reason for this trust revolves around two factors. First is the fact that it is a research project at CMU which is an institution they trust. When probed further, they mentioned that they would not trust such an intervention had they come across it in a different setting. A participant said:

*"...absolutely not. So this is a CMU building, I have a certain level of trust in the things that CMU puts out there in terms of what they're doing or what the researchers do, I know that there's IRB. If I go to like a shopping mall or in some other store or somewhere, and I see these devices, I am not going to be, as you know, trusting as I would be like let's say CMU building."*

Participant 67wZhi

Secondly, the fact that they have access to the researchers behind the project in the same building, so they could ask questions to learn more if they desired.

*"it's a privilege of the space...there's a sense of safety in just knowing that I could email [the creators] even if I never make the effort to do it. It makes you less angry or frustrated or feel like you're being taken advantage of."*

Participant kDiWCB

## Sensors not always noticeable

Even though all participants were aware of the presence of Mites sensors and had a visual reference of what they looked like, they hadn't noticed them in all areas. They had noticed them on the walls and on the plain white ceilings in the rooms they actively occupied, but some had completely missed them on the wood-slatted ceiling in the public areas of the first floor. This is understandable given the small size of Mites, the fact that it isn't the only sensor/ fixture on the ceiling and that it is much higher than the eye level while walking or sitting. It disappears into the building on this floor, as Weiser had envisioned (Weiser, 1999). But this raises an important question, does this give a false impression that this particular area is free of sensing or monitoring, especially if that might be a criterion for some occupants in the choice of what spaces they use?

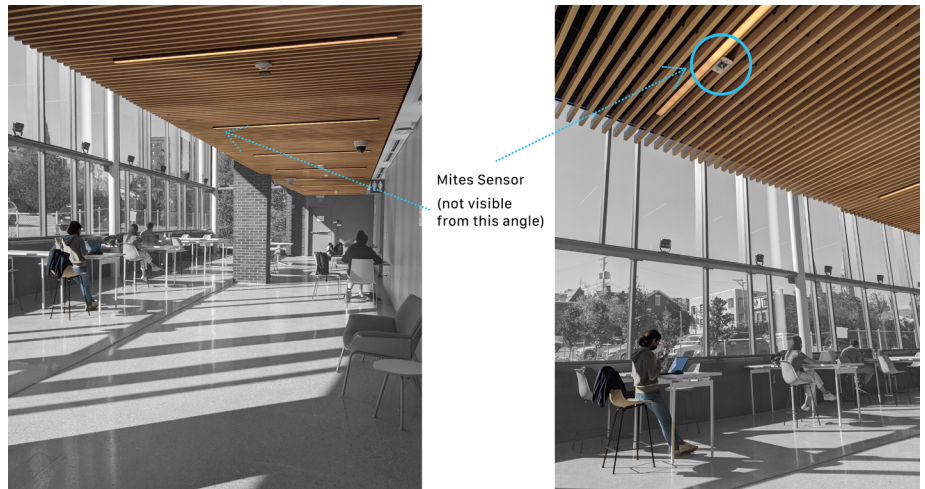


Figure 17: Mites are not noticeable on the wood-slatted ceiling in atrium and corridors

## Being in the shoes of the end-users

My participants had dual identities: engineers with sound technical knowledge than an average end user, and occupants/ end users at TCS with no say in the Mites project. Being in the shoes of the end-users gave them the distance from their identity as engineers and offered a more empathic perspective of what it means to live with technologies created by other engineers. One participant said:

*"...As engineers, to learn what it feels like to deal with these technologies, I think that we should be willing to actively sacrifice some of our privacy in this sort of puzzle because one day will be in a position of privilege, where we'll be building devices that other people don't understand as well as us, but are fundamental parts of their lives."*

Participant kDiWCB

### 6.3 DEVELOPED VALUES AND RESPECTIVE PRINCIPLES

The insights from the interviews were subsequently combined with secondary research and my motivation and posture as a Design Researcher (highlighted in the preface) to generate people-centered and place-centered privacy values. In line with VSD, I paid careful attention to the distinction between the personal values of the occupants and the moral values that would be relevant for the creators to think about at scale (Friedman, 1999). The privacy values that are produced as a part of this thesis are moral values and complemented by a definition. The key principle that guided the conceptualization and iteration of these was ensuring that the values are actionable for the creators yet open enough for them to think of data, and privacy, in a novel way. Therefore, the exact words and definitions published here were refined through four rounds of iteration using two strategies described as follows:

First, wherever possible, a large concept was broken down into its smaller components to make it specific and actionable. For example the need for transparency that all participants touched upon in one way or another, is broken into three values: 'purpose and practice', 'comprehension' and 'perceptibility'. Therefore the need for transparency is a principle that encompasses these three values.

Second and most importantly, the definition of each value is not a literal definition as per English language, rather it is a prompt to help creators think about the design of smart building systems in a manner that embeds privacy from the get-go. Answering these prompts can guide investigation and spark ideation (Desjardins, 2019) for engineers, designers, and architects. For example, the value of 'perceptibility' is defined as 'bring awareness to the hidden or less obvious presence of data sensing' which 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 following table shows the produced values with respective principles and the sources or insights that inspired them.

| Category or Principle  | Value Name          | Definition (framed as a prompt)  | Inspiration, Sources and Insights  |
|--|---------------------|--|--|
| Bring in the voice of occupants/end users                            | Empathy             | Be sensitive to the needs and perspectives of those implicated by the system | Feeling of Helplessness and being in the shoes of the end users: not having a say in the process and not fully comprehending the details of the technology made the participants reflect on their own position as engineers and creators |
|  | Participation       | Engage multiple stakeholder groups throughout the decision making process    | Feeling of Helplessness: stakeholders whose perspectives weren't included in the process felt uncomfortable and like test subjects   |
|  |                     |  | Participatory Design helps to equalize power among groups with unequal power and is a key value in Value sensitive design (Friedman and Kahn's review of Participatory Design, 2003)   |
|  |                     |  | Inviting stakeholder input can expand the perspective beyond that of designers and technologists and avoid the harms caused by exclusion of key stakeholder interests (Markkula Center for Applied Ethics)                               |
| Create IoT interventions that are specific to building use and place | Contextual          | Design details based on the needs of users of this environment               | Data is contextual, hence practices surrounding data must be, contextual too. (chapter 2)  |
|  | Culturally Situated | Account for the appropriate cultural values and norms                        | Privacy notions and behaviors vary with culture (Altman, 1975 expanding on the work of Alan Westin and anthropologists like Clifford Geertz and Dorothy Lee)   |
|  |                     |  | Privacy notions and behaviors vary with culture as noted by Altman (1975) and through personal observations  |
|  |                     |  | Privacy is a socio-cultural phenomenon therefore deeply entangled with cultural and organizational values that form the notion of a 'place'. (Dourish and Harrison, 1996)  |

|   |                      |   |   |
|---|----------------------|---|---|
| Create distinct data practices for public v/s private areas of the building | Differentiate        | Distinguish between data practices for private v/s public areas of the building | Finding anonymity in crowd and public spaces: occupants tend to move to more public spaces to talk about sensitive topics, which is the opposite of the common norm of expecting least amount of privacy in public. Therefore practices in shared contexts, where definitions of public and private exist with respect to each, norms of data collection needs re-interpretation. |
|   |                      |   | place can serve as useful guides for privacy (Dourish and Harrison, 1996)   |
| Enable Transparency for the occupants/ end users                            | Purpose and Practice | Clearly specify the purpose of data collection and data use practices           | Definition of 'Purpose specification' taken from OECD guidelines  |
|   |                      |   | Lack of Clarity on Purpose, Benefits and Data Practices: currently, it is unclear what use cases and data practices justify the collection of all the data  |
|   | Comprehension        | Explain purpose, practices and choices in a manner that users understand        | Lack of Clarity on Purpose, Benefits and Data Practices: the language used in the notice isn't clear to even students of privacy engineering who study the subject day in day out   |
|   | Perceptibility       | Bring awareness to the hidden or less obvious presence of data sensing          | Sensors not always noticeable   |
|   |                      |   | Not being able to see sensors can give a false impression of an area being free from surveillance and be deceptive  |

|   |             |   |   |
|---|-------------|---|---|
| Give Agency to the occupants/ end users                                 | Barriers    | Allow users the ability to temporarily disconnect from the IoT system   | Having access to a control mechanism of some sort and participate as desired empowers the users   |
|   |             |   | Having access to a control mechanism of some sort and participate as desired empowers the users   |
|   | Adaptation  | Enable users to adapt the IoT system to reflect their preferences       | Adaptability is what differentiates home from a house, from place to space. Just like arranging their homes and work stations helps people forge a connection, giving users the ability to personalize will give agency |
|   | Accessible  | Provide access to resources (person or other) for help and/or questions | Conflict between Trust and Discomfort: researchers of the project also work out of the TCS building and the occupants can talk to them if they wanted to  |
| 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 | Lack of Clarity on Purpose, Benefits and Data Practices: creates confusion, apprehensions and fears   |
|   | Foresight   | Consider the impact of IoT system on users and/or society over time     | "In the history of design and engineering, many avoidable harms and disasters have resulted from failing to adequately identify and appreciate the foreseeable ethical risks." (Markkula Center for Applied Ethics)     |
|   |             |   | Fear of normalization of 'surveillance': being surrounded by sensors everywhere all the time could lead to de-sensitization towards their presence and loss of ability to care about privacy.                           |



|   |                |  |  |
|---|----------------|--|--|
| Take responsibility for outcomes and comply with measures to address concerns | Accountability | Create mechanisms to ensure compliance and addressing user concern | <p>Combination of</p> <ol style="list-style-type: none"> <li>1. Be proactive about developing policies, procedures, and software that will support compliance with these principles (definition of Accountability cited by Cranor based on OECD guidelines, 2003).</li> <li>2. FIPPS (Fair Information Practice Principle) called 'Self-Regulation' under Enforcement</li> </ol> |
|---|----------------|--|--|

## 6.5 A NOTE ON EMPATHY

On the surface it seems like a cliché to include Empathy and there are good arguments for how empathy by itself is not enough for good design. However, the decision to include this was rooted in the realization that it is still an undermined value in purely engineering-driven philosophies. This realization stood out through a stark contrast between the argument ‘they are concerned because they don’t understand the technology fully’ and the perspective of those who live with these technologies on a daily basis without any say in it whatsoever. While it is true that an average end user or occupant of a Smart workspace may not ‘fully understand’ the technology, the question is why would that be more important than its impact? Besides, the argument is problematic because:

- Understanding technology fully does not guarantee that it is in the best interest of the people who are implicated by it.
- It perpetuates the ‘tech for tech sake’ narrative where engineering marvel is given precedence over a human-centered perspective for innovation.
- My research participants had sound technical knowledge as compared to an average end-user/occupant. The fact that they were not involved in the project gave them distance from the exact technical details and brought out the disconnect between vague intentions of such ubiquitous technology and what it means for the lived realities of people.

In the same regard, it is also important to highlight that ‘Empathy’ is not a phase or a step to be performed in the process, but rather it is a value that should underpin any such intervention, starting from its conception to execution and ripple out to the decisions during active functioning. This demands a mindset shift where there is a clear difference between empathy in itself and ‘doing’ empathy.



## 6.5 PRELIMINARY TEST OF VALUES THROUGH A WORKSHOP

### Workshop Structure

After creating the privacy values, I conducted a 90 minutes generative workshop with 6 privacy engineers (3 teams of 2 each) to test how the values might be received, and used. In order to get true reactions, the participants weren't primed towards privacy or privacy values at the beginning and were told that the goal of the workshop was for them to come up with IoT application ideas for TCS independently of Mites. The framing of the workshop around ideation was a conscious choice for simulating a process close to how most IoT ideas are conceived, where considerations of privacy surface only once there is clarity on questions around data. The other deliberate decision was guiding the teams based on a human-centered design process where the needs of users precede sensors and technology. The process had two distinct parts:

- **Part 1: User hat (20 minutes):** The participants were asked to reflect on their needs and aspirations from a workspace like TCS, pick the most pressing need that may be solved by data and think of ideas to address it. Since they were expected to think like a user, they were told to not worry about the feasibility of the idea.
- **Part 2: Creator hat (40 minutes):** Here, they were asked to don the hat of a creator who has been handed rough ideas for something that the users of TCS might find helpful. The task was to refine these ideas by thinking of all the stakeholders involved and how it might impact them, the data needed to make this feasible, and privacy values that would respond to the impact on stakeholders due to data collection and processing.

During Part 2, the teams were handed printouts for examples of relevant stakeholders, data plus sensor, and privacy values. They could use these or write their own if they saw fit. These two exercises were followed up with team share out and group discussion for 20 minutes, and a 5-minutes individual survey. This 20 minutes discussion helped bring out participants' reflections on the process and was the crux of the workshop.

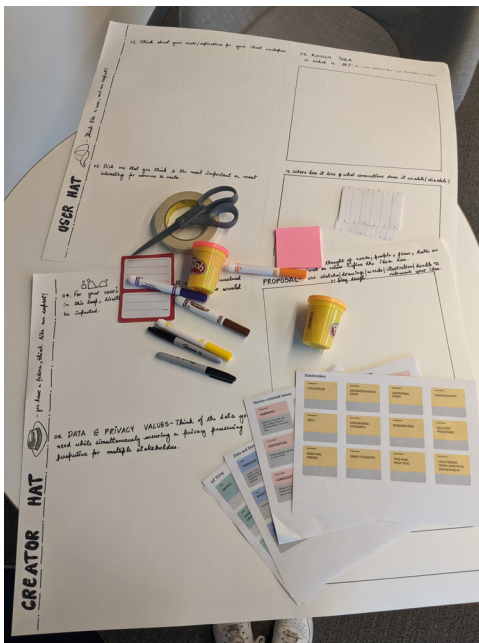


Figure 19: Worksheets for participants, part 1: user hat and part 2: creator hat (or federal)



Figure 20: Participants engaged in workshop activities



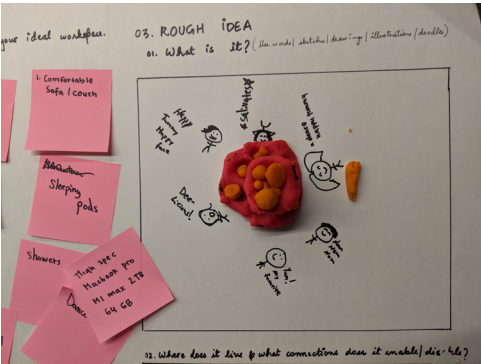


Figure 20: Star-trek food replicator made by the team with Play-Doh

Workshop artifacts and props

Each team was given A0 size worksheets for each part along with post its, markers, and Play-Doh (fig 19). There was visible excitement on seeing the Play-Doh and two out of the three teams used it during their process. The worksheets were hand-written instead of being printed so that all the natural imperfections of a handwritten document helps create a sense of comfort for the participants to write, draw, sketch or scribble on. While these choices were ordinary on the surface, they were remarked as new and refreshing by the participants in making sense of how different parts of the idea related to each other.

Workshop Insights:

The following four insights stood out from the workshop and informed the design of a suitable intervention:

Mixed opinions on being given a menu of Values.

Participants had differing opinions on being assigned a menu of values to choose from. While one participant noted:

*"...the step for picking data and privacy values was tricky, it felt like a lot of privacy things should apply but also hard to fit it in."*

Another participant said:

*"...I liked the mix of open-ended and predetermined values, but maybe all of them could apply. The same goes for stakeholders, so maybe ask us to pick a set."*

Figure 21: Menu of privacy value assigned during the workshop along with blank tiles

| Human-centered Values  |  | Place-centered Values  |  | Data-centered Values   |                          |                          |
|--|--|--|--|--|--------------------------|--------------------------|
| <div>Privacy Value</div> <div>HARMONY</div> <div>Balances the benefit with risks, whether they are potential, likely or less likely risks.</div> | <div>Privacy Value</div> <div>PERCEPTION OF BENEFIT</div> <div>Benefit of the thing/system and data practices obvious and clear to the user.</div>             | <div>Privacy Value</div> <div>DIFFERENTIATION</div> <div>Has distinct data practices for private v/s public areas of the building.</div> | <div>Privacy Value</div> <div>CULTURALLY SITUATED</div> <div>In alignment with cultural values of the organization or the wider context.</div> | <div>Privacy Value</div> <div>ANSWERABILITY</div> <div>Explicitly states resources (people or other) for help and/or questions.</div>        | <div>Privacy Value</div> | <div>Privacy Value</div> |
| <div>Privacy Value</div> <div>CONTEXTUAL</div> <div>Details designed specifically for this context.</div>  | <div>Privacy Value</div> <div>EMPATHY</div> <div>The ability of creators to understand the perspective of users during the design and development phase.</div> | <div>Privacy Value</div> <div>BARRIERS</div> <div>Allowing users to temporarily disconnect themselves from the thing/system.</div>       | <div>Privacy Value</div> <div>ADAPTATION</div> <div>Ability of users to adapt the thing/system to forge a connection.</div>                    | <div>Privacy Value</div> <div>DEMOCRACY</div> <div>Involves multiple stakeholders in the decision making process.</div>                      | <div>Privacy Value</div> | <div>Privacy Value</div> |
| <div>Privacy Value</div> <div>FORESIGHT</div> <div>Taking into account how the thing/system might impact users or society over time.</div>       | <div>Privacy Value</div> <div>COMPREHENSIBLE</div> <div>Purpose, practices and choices explained in a manner understood by the users.</div>                    | <div>Privacy Value</div> <div>PERCEPTIBLE</div> <div>Bringing awareness to the hidden or less obvious presence of data sensing</div>     | <div>Privacy Value</div>   | <div>Privacy Value</div> <div>TRANSPARENCY</div> <div>The purpose of data collection and data practices clearly specified or embodied.</div> | <div>Privacy Value</div> | <div>Privacy Value</div> |

**Seeing data from a different perspective.**

This group of participants often works with intricacies of the data itself (from a technical and/ or managerial perspective) or around transparency through usability. However, this process opened them up to a different point of view, one that is focused on 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."*

**Values helped in thinking beyond software.**

During the open discussion, I used one of the privacy values called 'Barriers' to highlight how the closing of a door is a commonly recognized gesture for expecting privacy, but similar analogies are hard to come by in IoT applications. Too often, the mechanisms that allow users to temporarily disconnect are either independent interventions designed after the fact or are creative manipulations done by the users. They are rarely an integral part of the design of that ecosystem. This example resonated well with the participants and sparked an interesting discussion about metaphors like 'pulling the plug' or laptop webcam covers that are only now becoming an integral part of laptops. As the discussion proceeded, they acknowledged the importance of thinking more broadly than mere software assurances for privacy.

The participant who had earlier expressed difficulty in working with privacy values was inspired by the effectiveness and simplicity of 'Barriers' and said:

*"...future technology would probably benefit from performing physical actions to indicate privacy...it would be good to consider (barriers) in future design rather than small software guarantees for what data would be collected or used for."*

### **Pessimism for Technology.**

As privacy engineers, these individuals are constantly working to fix what has either already gone wrong or could potentially go wrong, which sometimes makes them feel pessimistic about technology.

One of the participants recognized the complexity of the entire process (like monetizing IoT and other technology projects) but found it refreshing to think about the front end of the design and development process in a manner that integrates needs, stakeholders and values.

*"...I feel like I'm always trying to stop bad things from happening instead of thinking what if we create something that isn't going to do bad things."*

All these insights helped in drawing two conclusions, first that bringing a broader perspective definitely opened up my audience to a different, and a more human-centered, way of conceptualizing privacy. However, some of them paid close attention to the values only after we started discussing them through tangible examples. The manner in which the values were represented and conveyed missed the mark in being approachable for my audience during the process. This led to a formal design exercise for making privacy values more tangible and approachable.

## 6.6 MAKING VALUES APPROACHABLE THROUGH DESIGN

To make each value easily understandable and more directly applicable in the design process, I leveraged the use of metaphors. The use of metaphors is a common practice for idea generation in design, but most importantly, metaphors can transcend the boundaries of professional disciplinary knowledge (Saffer, 2005). Metaphors, by their very nature, 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 cited by Saffer, p.6). Therefore, the use of metaphors would allow making values relatable for an interdisciplinary group of audience while simultaneously leaving room for them to leverage their individual knowledge. This also complements the definition of each value framed as an ideation prompt as opposed to a literal definition (section 6.3). 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 that is hidden in plain sight in the crowd but is noticeable due to his distinct manner of clothing and hair. To make data sensing more noticeable, three different professionals can address this in three different ways: an architect may propose to place all sensors at eye level, an engineer may propose an app that triggers a notification when in the vicinity of sensors and a designer may come up with an impeccable communication design for a notice.

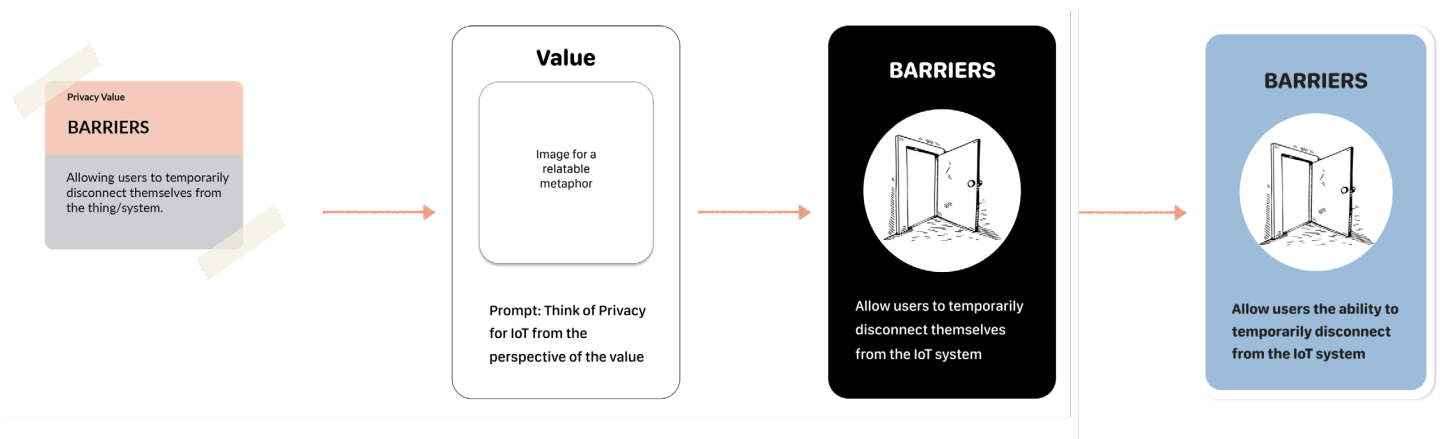
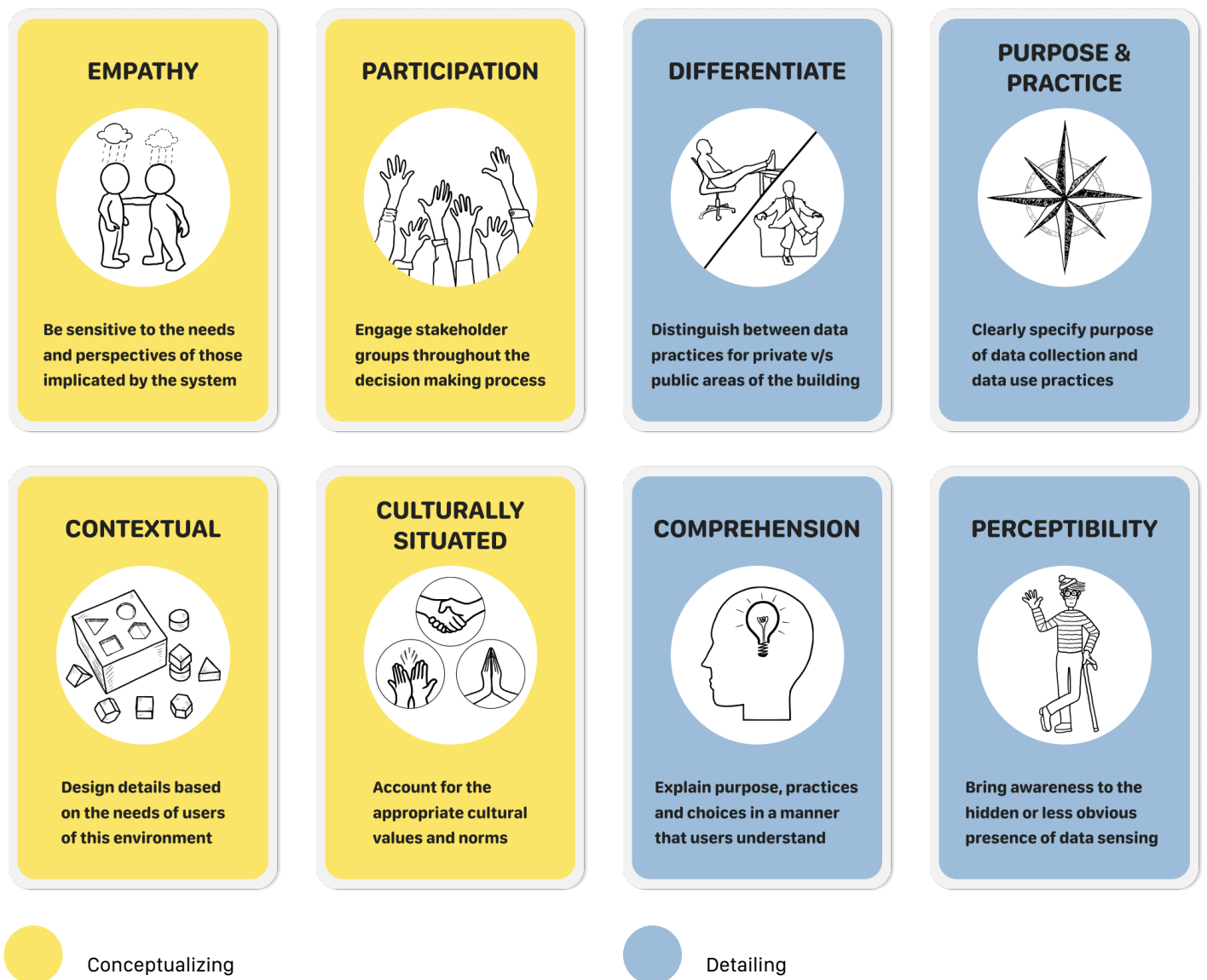


Figure 22: The values evolved in terms of the presentation through the use of a metaphor and color coding based on stages of a design process



This design structure of the privacy values with the value name, image of a metaphor and a prompt naturally lent itself to a card format. To make the value cards usable by creators, these have been color-coded as per three broad phases of a design process: Conceptualizing (yellow), Detailing (blue) and Refining (orange). The color-coded cards can be printed by creators as part of a toolkit described in the next chapter.

Figure 23: Fourteen color-coded value cards





### BARRIERS



Allow users the ability to temporarily disconnect from the IoT system

### ACCESSIBLE



Provide access to resources (person or other) for help and/or questions

### ADAPTATION



Enable users to adapt the IoT system to reflect their preferences

### ACCOUNTABILITY



Create mechanisms to ensure compliance and addressing user concern

### 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



Refining

## CHAPTER 7.

# **DESIGN IMPLEMENTATION**

The seven core principles and the fourteen value cards produced in this research can be accessed by creators through a privacy toolkit or an online platform. The toolkit is available as a Pdf file format on the platform. Although I conducted primary research with privacy engineers, the resultant values, toolkit and the platform are suited for an interdisciplinary group of creators who shape the smart workspaces, whether they are architects, engineers, designers or building managers etc. Traditionally, each of these diverse sets of professionals have a unique area of focus. For example, designers and architects focus on the occupants' experience, engineers focus on the technical details, and building managers focus on efficient functioning of the building. However, the final outcome is a cumulative product of the big and small decisions made by them, including the ones that impact privacy. Therefore, it is important to tie all these seemingly disparate decisions together by fostering an interdisciplinary dialogue among these professionals to think of data, people and place simultaneously for privacy. The toolkit or the platform would enable this dialogue.

The design of the toolkit and the online platform varies slightly to fit each format appropriately. However, both are designed to open up privacy considerations early on and serve as ideation tools for participating professionals. They are not intended to replace the existing processes for any of these professionals, rather they are meant to complement that process by helping to make timely accommodations. For example, if an architect proposes to place all sensors at eye level to make data sensing more obvious to occupants, she would have to plan for the exact placement in her design. This decision would need to become an important part of her design brief since it is linked with the electrical circuitry as well as the interior aesthetics. On the other hand, an engineer's proposal to create an app to notify occupants when in the vicinity of sensors may come down the road, but also means that resources would have to be set aside from the overall budget. The most appropriate solution would then depend on considerations of the overall project and would be best planned in advance collectively. Thus, this sort of collective ideation early on can certainly help to embed privacy as a forethought and integrate them into the existing individual workflows of the team members.

## 7.1 PRIVACY DESIGN TOOLKIT FOR SHARED SMART WORKSPACES

### Format

The toolkit is designed for letter-sized landscape orientation so that it can be easily printed for use if needed. It integrates two formats: i) filling out as a workbook by an individual if they are working alone or asynchronously with the team, ii) printable value cards and a guide on how to use them for in-person team ideation.

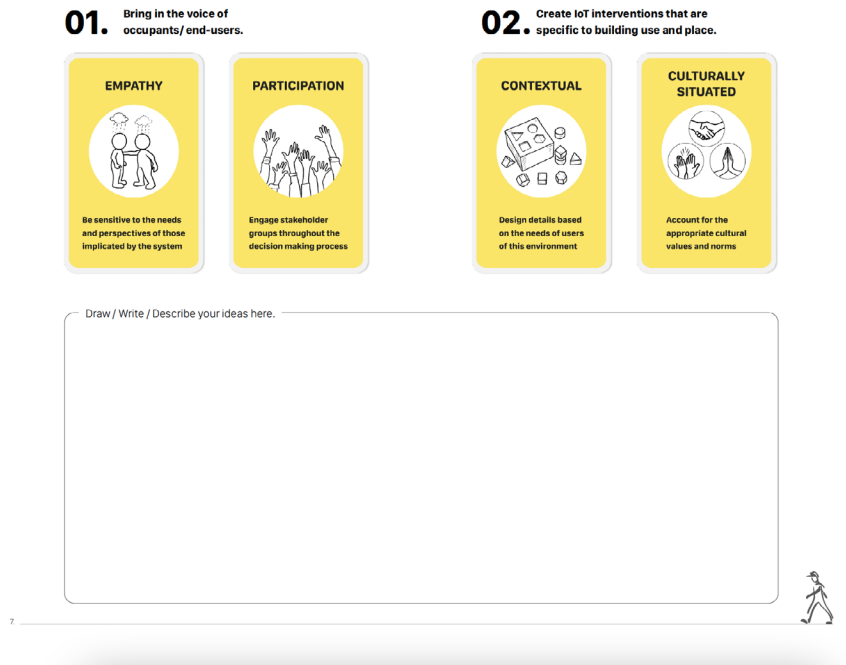


Figure 24: Workbook format in the toolkit

### Recommended instructions

This is represented as a diagram to give basic instructions in a visual format. The visual format is also apt in emphasizing that the use of this toolkit shouldn't be seen as a one time activity in a linear process, but something that the interdisciplinary team should return to periodically as the project evolves. It is ideal to start using these prompts early on in the process, but since this may not always be possible, the recommendation is to always make the first ideation attempt collectively with members from different professional backgrounds. This would help in cross-mapping ideas easily based on the stage everyone is at and provide a useful starting point for subsequent collaboration.

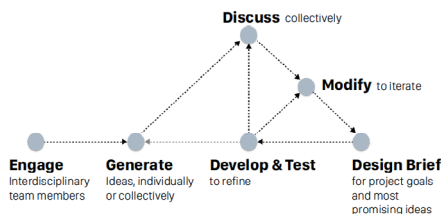


Figure 25: Recommended instructions in the toolkit

## Prompts

To help creators focus on the phase most applicable to them at the time of using the toolkit, the principles and prompts are provided in a color-coded format as per three categories: Conceptualizing (yellow), Detailing (blue) and Refining (orange). There is a table that gives an overview of these principles and prompts followed by each of them individually.

## Identifying the Scope

The creators are encouraged to identify the scope of the project through two key activities:

Thinking about the occupants and their needs: This includes questions like who will occupy this space permanently? What would they be doing in this space? Have you spoken to them about what they need or would find useful in this space? Are there going to be visitors?

Knowing the team: This would be captured through the question for listing all the collaborators engaged in the process.

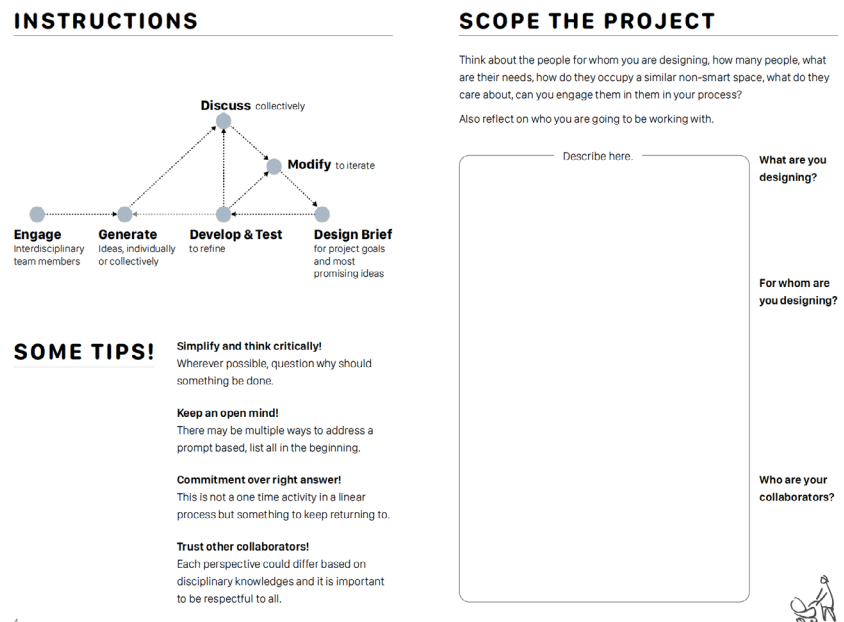



Figure 26: Scoping the project (right side)

Design brief

The design brief is a one-page summary of the identified scope and the ideas generated by the creators (or the individual) through the use of the toolkit. The creators fill it collectively at the end. The reason to design this as a summary is so that this one-page artifact can serve as a useful reminder of the project goals for everyone. Additionally, just as project briefs evolve with the progression of the project, this design brief should evolve as well. Subsequent iterations of this brief can also serve as a useful documentation for the project.



PROJECT NAME:

I/we are designing \_\_\_\_\_ for \_\_\_\_\_  
\_\_\_\_\_ keeping in mind \_\_\_\_\_  
\_\_\_\_\_

The overarching goals for the project are to \_\_\_\_\_ and in order to make it  
privacy-preserving, the project would be made contextual by incorporating ideas like \_\_\_\_\_  
\_\_\_\_\_, the purpose and data practices would be clearly specified by \_\_\_\_\_  
\_\_\_\_\_ and participation of end occupants would be invited \_\_\_\_\_  
\_\_\_\_\_

In addition, the IoT system tries to include privacy considerations through specific details like \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Date:

Figure 27: Design brief generated as a result to using the toolkit

## 7.2 AN ONLINE PLATFORM FOR DESIGNING WITH PRIVACY

The 'Designing with Privacy' platform is envisioned to be the larger ecosystem that includes the toolkit as a part of it. In its current state, it is only a proposal and relevant for future work. Similar to the toolkit, it is meant to aid in ideation by the interdisciplinary teams but has three additional features:

It supports real-time collaboration between remote teams by virtue of being online. If made interoperable with whiteboard tools like Mural or Miro, it'll also help to create living documents for each of the projects.

It helps connect peers and professionals with a larger community using the platform,

It acts as a knowledge repository for ideas tried by the community members.

Together, these three features would elevate the usefulness of the principles and values for a wider community and spread the word for the alternative narrative for privacy for smart buildings. A prototype of the platform can be accessed through <https://ishahans.com/project/penumbra-of-privacy>

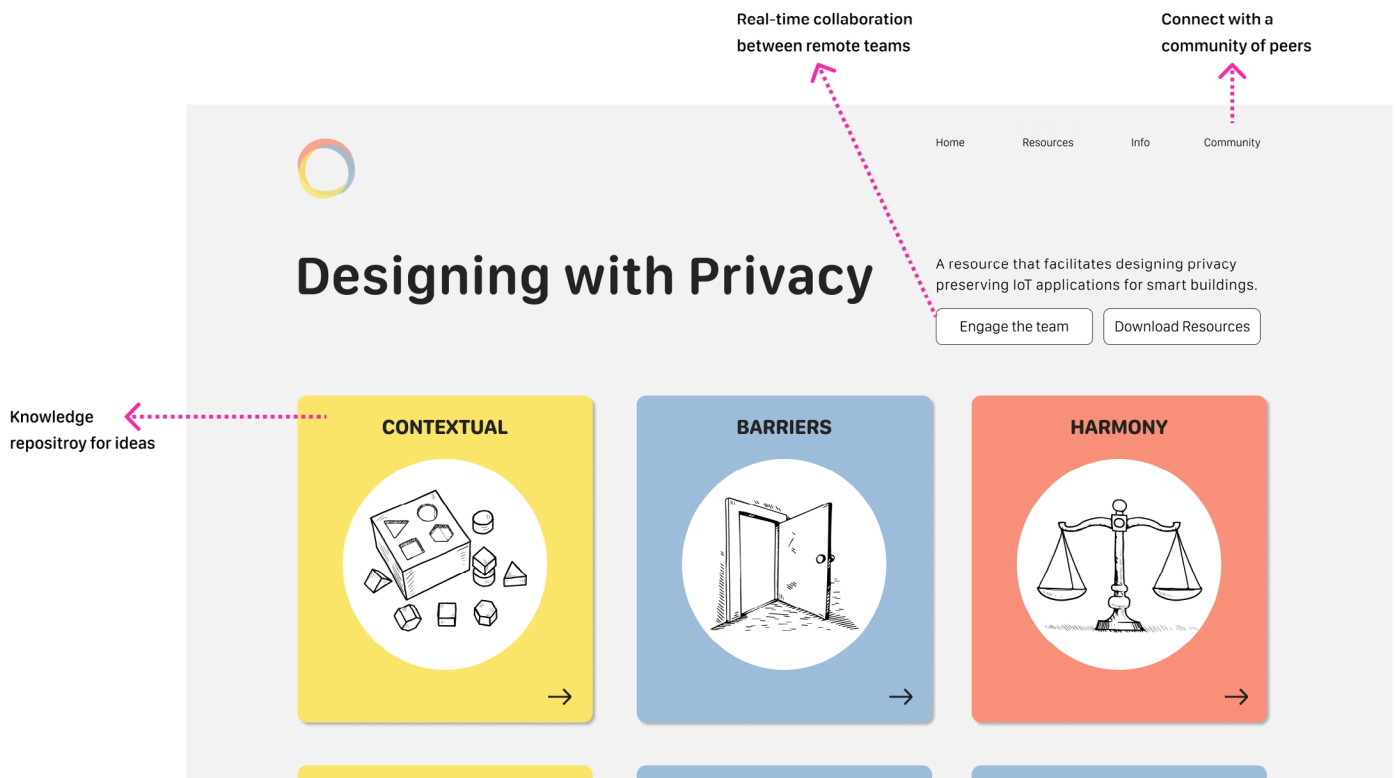


Figure 28: Online Platform proposal

*PART III: CONCLUDING REMARKS*

CHAPTER 8.  
**CONCLUSION**



This thesis aims to go beyond the status quo of current privacy practices, or the umbra, and create a broader approach for smart workspaces based on human-centered experience and values, or the penumbra. The umbra of current privacy practices is heavily skewed towards software and data management perspectives, with minimal focus on people, place and the associated values. To create this penumbra, I first propose two reframings: 1) combining a people-centric and place-centric perspective for privacy with a computing perspective, 2) creating preventative approaches instead of remedial ones by embedding people-centric and place-centric privacy values in the front end of the design process for creators. The primary research conducted based on these re-framings demonstrated that focusing on people and place centered values at the front end of the design process sparked greater empathy and hope in creators. It helped them visualize people in a place from the perspective of their day to day lives without reducing them to data in a strictly algorithmic sense. This human-centered perspective also relieved them of the pessimism around technology and provided hope that more deliberation early on in the innovation process can reduce the burden for ‘fixing’ technology after the fact.

The insights from this investigation have produced seven privacy principles and fourteen values suitable for shared contexts in the non-domestic realm. These principles and values can be accessed by creators through Privacy design toolkit (described in section 7.1) and, in the future, through Designing with Privacy platform (described in section 7.2). The values have been strategically framed as ideation prompts to ingrain privacy considerations early on, thereby strengthening a preventative approach.

In a general sense, this thesis also pushes back on the narrative of conceptualizing smart buildings as computers. It proposes a new intermediate level theory of weaving people, place and data explicitly in the context of smart buildings. In doing so, it contributes to the larger privacy discourse through the creation of a novel approach better suited for smart buildings. The robust foundation laid through this work can be built upon through two future directions: testing the toolkit in practice, and developing and testing the ‘Design with Privacy’ platform. The toolkit is proposed to be used in the near future in suitable classes at Carnegie Mellon University, so that the soon to be professionals can be exposed to these ideas during their academic training. The hope is that by practicing this manner of thinking, they would be prepared to design for, and with, privacy in a more human-centered manner.

## CHAPTER 9.

# **PERSONAL REFLECTION**

This work has been two and a half years in the making and is inspired by my motivation to critically reflect on the tech-first perspectives. I have learned a great deal about privacy, but most importantly I have learned a lot about bridging the gaps. The hardest, and also the most interesting, part of this journey has been the lack of a shared vocabulary between different disciplinary perspectives. As a former practicing architect, current designer interested in emerging technology who has been working with privacy engineers, I have come to realize that these vocabularies are deeply linked with different mental models associated with specific disciplinary backgrounds. It is perhaps for this reason that my work is full of metaphors to help bridge these gaps, both in the tangible output (like the value cards) as well as in the framing of my work (like the title). I have fallen and risen multiple times in this process and even felt frustrated at times, but have also felt really inspired by the conversations with professionals across disciplines. Reflecting on these conversations has helped me draw the connections that have resulted in this work, some of which were captured in my thesis journal on Medium from September - December 2021. There are new ideas brewing in my head for how to take this work further and create an impact on what is termed as the 'real world' outside of academia, a place where I believe bridging gaps is important. I hope that this inspires others to push the boundaries of what we know, how we think and how we can question our own perspectives to integrate a different one.

## REFERENCES

- Alan Westin is the father of modern data privacy law | Articles. (2021, January 15). Osano. <https://www.osano.com/articles/alan-westin#:~:text=Westin%20is%20perhaps%20best%20known,the%20field%20of%20privacy%20law>
- Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding* (First Printing ed.). Brooks/Cole Pub. Co.
- Borgman, C. L. (2017). *Big Data, Little Data, No Data: Scholarship in the Networked World* (Reprint ed.). The MIT Press.
- Brachmann, S. (2018, July 14). Warren Johnson, Father of Thermostats and Room Temperature Control. IPWatchdog.Com | Patents & Patent Law. Retrieved May 7, 2022, from <https://www.ipwatchdog.com/2018/07/16/warren-johnson-father-thermostats-room-temperature-control/id=99351/>
- Bridle, J. (2018). *New dark age: Technology and the end of the future*. Verso Books.
- 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](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972)
- Cavoukian, A. (2022). *Privacy by Design: Take the Challenge*. Ann Cavoukian.
- Coles-Kemp, L., Jensen, R. B., & Heath, C. P. R. (2020). Too Much Information: Questioning Security in a Post-Digital Society. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. <https://doi.org/10.1145/3313831.3376214>
- Cranor, L. F. (2004). I Didn't buy It for Myself. *Designing Personalized User Experiences in eCommerce*, 57–73. [https://doi.org/10.1007/1-4020-2148-8\\_5](https://doi.org/10.1007/1-4020-2148-8_5)
- Cranor, L. F., & Garfinkel, S. (2005). *Security and Usability: Designing Secure Systems that People Can Use* (1st ed.). O'Reilly Media.
- 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*, 1–13. <https://dl.acm.org/doi/abs/10.1145/3290605.3300581>
- Eric, T. (2019, May 14). *How the Internet of Things Benefits Building Operations* [ebook]. PlanGrid Construction Productivity Blog. Retrieved May 7, 2022, from [https://blog.plangrid.com/2019/05/internet-of-things-for-building-operations/?doing\\_wp\\_cron=1651950181.5089550018310546875000](https://blog.plangrid.com/2019/05/internet-of-things-for-building-operations/?doing_wp_cron=1651950181.5089550018310546875000)
- Erickson, T. D. (1995). Working with Interface Metaphors. *Readings in Human-Computer Interaction*, 147–151. <https://doi.org/10.1016/B978-0-08->

051574-8.50018-2

- Fox, M. (2013, February 23). Alan F. Westin, Who Transformed Privacy Debate Before the Web Era, Dies at 83. The New York Times. <https://www.nytimes.com/2013/02/23/us/alan-f-westin-scholar-who-defined-right-to-privacy-dies-at-83.html#:~:text=22%2C%202013-,Alan%20F.,was%20cancer%2C%20his%20family%20said.>
- Friedman, B. (1997). Human values and the design of computer technology (ed.). Center for the Study of Language and Information, USA.
- Friedman, B., & Hendry, D. G. (2019). Value Sensitive Design: Shaping Technology with Moral Imagination (Illustrated ed.). The MIT Press.
- Friedman, B., & Kahn, P. H. (2002). Human values, ethics, and design. The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies and Emerging Applications, 1177–1201. <https://dl.acm.org/doi/10.5555/772072.772147>
- Friedman, B., Kahn, P. H., & Borning, A. (2002). Value Sensitive Design: Theory and Methods. University of Washington Technical Report, 2, 12. <https://www.semanticscholar.org/paper/Value-Sensitive-Design%3A-Theory-and-Methods-Friedman-Kahn/54bfbe5a886807bf3b80cdd201a7140eaf26ad70>
- Furnish, T. A. (2007, September 3). Motion Sensors – USC Viterbi School of Engineering. Illumin Magazine. Retrieved May 7, 2022, from <https://illumin.usc.edu/motion-sensors/>
- Gellman, R. (2014). Fair Information Practices: A Basic History - Version 2.22. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.2415020>
- Greenfield, A. (2006). Everywhere: The Dawning Age of Ubiquitous Computing (1st ed.). New Riders Publishing.
- Harari, Y. N. N. (2019). 21 Lessons for the 21st Century (Reprint ed.). Random House Publishing Group.
- Harrison, S., & Dourish, P. (1996). Re-place-ing space. Proceedings of the 1996 ACM Conference on Computer Supported Cooperative Work - CSCW '96. <https://doi.org/10.1145/240080.240193>
- Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W. (2009). A “nutrition label” for privacy. Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09. <https://doi.org/10.1145/1572532.1572538>
- 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.
- Mattern, S. (2021). *A City Is Not a Computer: Other Urban Intelligences* (Places Books, 2). Princeton University Press.
- McDonald, A. M., & Cranor, L. F. (2008). The Cost of Reading Privacy Policies. *A Journal of Law and Policy for the Information Society*, 4(3), 543–568.
- McEwen, A., & Cassimally, H. (2013). *Designing the internet of things* (1st ed.). John Wiley & Sons.
- Proshansky, H. M., Ittelson, W. H., & Rivlin, L. G. (1970). *Environmental psychology: man and his physical setting*. New York: Holt, Rinehart and Winston.
- Saffer, D. (2005). *The Role of Metaphor In Interaction Design* (Master's thesis ed.). Carnegie Mellon University.
- Sauter, M. (2018, February 13). Sidewalk Labs: Google's Guinea-Pig City in Toronto. *The Atlantic*. Retrieved May 7, 2022, from <https://www.theatlantic.com/technology/archive/2018/02/googles-guinea-pig-city/552932/>
- Schaub, F., & Cranor, L. F. (2020). Usable and Useful Privacy Interfaces. *An Introduction to Privacy for Technology Professionals*, 176–299.
- Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2171018](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018)
- The Secret Life of Big Data | Intel. (2014, February 28). YouTube. <https://www.youtube.com/watch?v=CNoi-XqwJnA>
- Wang, T. (2017, July 19). The human insights missing from big data. TED Talks. [https://www.ted.com/talks/tricia\\_wang\\_the\\_human\\_insights\\_missing\\_from\\_big\\_data](https://www.ted.com/talks/tricia_wang_the_human_insights_missing_from_big_data)
- Weiser, M. (1999). The computer for the 21st century. *ACM SIGMOBILE Mobile Computing and Communications Review*, 3(3), 3–11. <https://doi.org/10.1145/329124.329126>
- Westin, A. (1967). *Privacy and Freedom*. Atheneum.

## APPENDIX



# PRIVACY DESIGN TOOLKIT FOR SHARED SMART SPACES

---



# ABOUT

---

This toolkit is to aid in ideation for:

**...Engineers,**

**...Technologists,**

**...Architects,**

**...Designers,**

**...& anyone working on shared Smart Workspaces,**

to embed privacy considerations from  
the start using value-based prompts.

This toolkit is designed to help creators like yourself practice a preventative approach to privacy while creating shared smart workspaces. It facilitates ideation based on people-centered and place-centered privacy values. It is ideal to use the toolkit in an interdisciplinary capacity with other professionals on the project to bring a rich diversity of ideas from different disciplinary perspectives concerned with buildings.

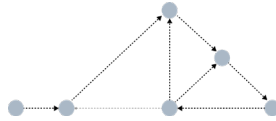
This toolkit is developed based on research conducted for privacy for smart workspaces as part of Master of Design thesis at Carnegie Mellon University. There are 14 value-based prompts grouped under 7 principles which should be used throughout the design and development process of your project. The value and principles are relevant other shared contexts in the non-domestic realm too and may even be useful for the domestic context with critical reflection and adaptation.



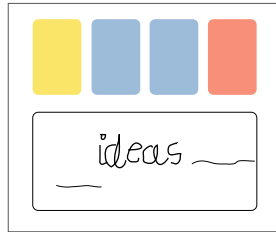
# TOOLKIT CONTENTS

---

Recommended use  
Instructions



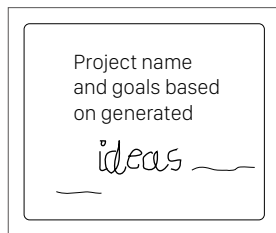
Principles and Prompts  
in a workbook format



Printable prompt cards



Design Brief



Link to Resources

<https://ishahans.com/project/penumbra-of-privacy>

# BEFORE STARTING

---

**When to use:**

1. At the beginning when all details are at a conceptual stage.
2. Return to it periodically as the project progresses, or at crucial decision making junctures.

**Who should participate:** It is ideal to use the toolkit in an interdisciplinary capacity by bringing together all different professionals on the project, like engineers, architects, designers, building managers etc. The way the project shapes is a cumulative outcome of the big and small decisions made by all of these professionals, including the ones that impact privacy. Bringing everyone together for ideation early on can help to brainstorm ideas from a rich diversity of perspectives and make accommodations as the project progresses.

In the absence of an interdisciplinary team, this toolkit can also be used by an individual independently.

**How to prepare:**

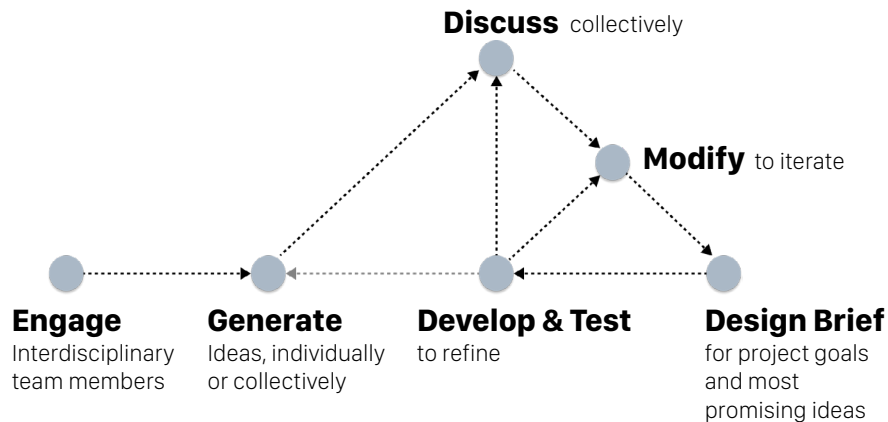
If done individually, fill out pages 7-12 as a workbook.

If done collectively as a team, the facilitator should:

- Print the prompt cards and facilitate the whole activity.
- Print the design brief to be filled by the team at the end.
- Create and distribute copies of the design brief to participating members.



# INSTRUCTIONS



## SOME TIPS!

### **Simplify and think critically!**

Wherever possible, question why should something be done.

### **Keep an open mind!**

There may be multiple ways to address a prompt based, list all in the beginning.

### **Commitment over right answer!**

This is not a one time activity in a linear process but something to keep returning to.

### **Trust other collaborators!**

Each perspective could differ based on disciplinary knowledges and it is important to be respectful to all.

# SCOPE THE PROJECT

Think about the people for whom you are designing, how many people, what are their needs, how do they occupy a similar non-smart space, what do they care about, can you engage them in them in your process?

Also reflect on who you are going to be working with.

Describe here.

**What are you designing?**

**For whom are you designing?**

**Who are your collaborators?**



# PRINCIPLES AND PROMPTS

---

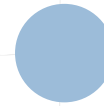
**There are 7 core principles and 14 value-based ideation prompts.**

These are divided into three categories:



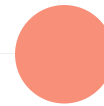
## **Conceptualizing**

These values will help to ground your project no matter the stage you or your team are at.



## **Detailing**

These values will aid in articulating specific details for your IoT system.



## **Refining**

These values will serve as guardrails for your project to ensure ethical innovation.

Three key values that must be responded to irrespective of the stage of your project are 'Purpose and Practice', 'Contextual' and 'Participation'. Together, these three values will help to ensure a people-centered and place-centered point of view.



| S. No. | Principle   | Value                | Prompt  |
|--------|---|----------------------|---|
| 01.    | 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       |
| 02.    | 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                           |
| 03.    | 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 |
| 04.    | 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          |
| 05.    | 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         |
| 06.    | 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             |
| 07.    | Take responsibility for outcomes and comply with measures to address concerns.          | Accountability       | Create mechanisms for ensuring compliance and addressing user concern           |



## 01. Bring in the voice of occupants/ end-users.

### EMPATHY



Be sensitive to the needs and perspectives of those implicated by the system

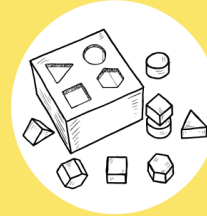
### PARTICIPATION



Engage stakeholder groups throughout the decision making process

## 02. 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

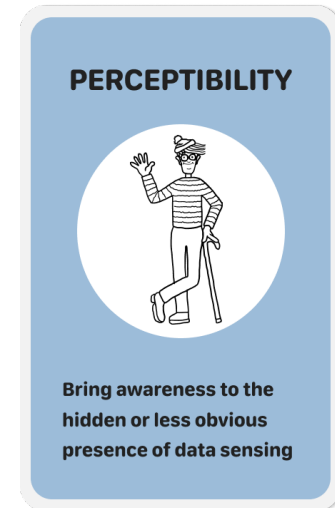
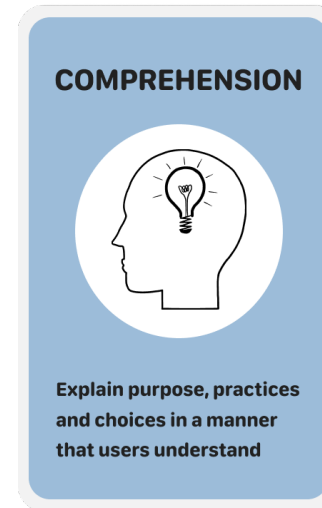
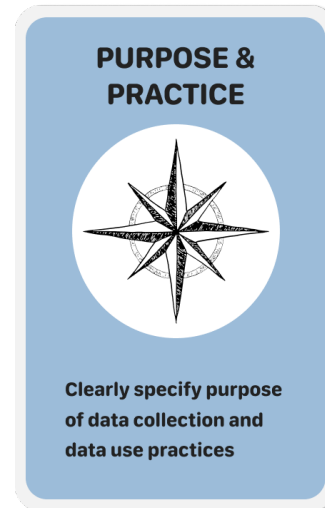
Draw / Write / Describe your ideas here.



## 03. Differentiate data practices for public v/s private areas.



## 04. Enable Transparency for the occupants/ end users.



Draw / Write / Describe your ideas here.





## 05. Give Agency to the occupants/end users.

### BARRIERS



Allow users the ability to temporarily disconnect 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

Draw / Write / Describe your ideas here.



## 06. 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

## 07. Take responsibility for outcomes and comply with measures to address concerns.

### ACCOUNTABILITY



Create mechanisms to ensure compliance and addressing user concern

Draw / Write / Describe your ideas here.



# DESIGN BRIEF

---

**Prioritize ideas from the ideation and make a design brief.**

Whether made individually or collectively, the brief will help the entire team work towards privacy through a collective vision.





## PROJECT NAME:

I/we are designing \_\_\_\_\_ for \_\_\_\_\_  
\_\_\_\_\_ keeping in mind \_\_\_\_\_  
\_\_\_\_\_.

The overarching goals for the project are to \_\_\_\_\_ and in order to make it  
privacy-preserving, the project would be made contextual by incorporating ideas like \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_, the purpose and data practices would be clearly specified by \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_ and participation of end occupants would be invited \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_.

In addition, the IoT system tries to include privacy considerations through specific details like \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_.

Date:

# **PRINTABLE PROMPT CARDS**

---



## EMPATHY



Be sensitive to the needs and perspectives of those implicated by the system

## PARTICIPATION



Engage stakeholder groups throughout the decision making process

## DIFFERENTIATE



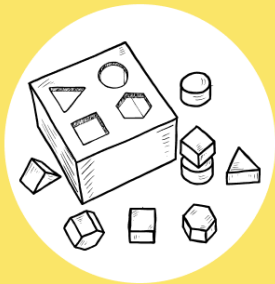
Distinguish between data practices for private v/s public areas of the building

## PURPOSE & PRACTICE



Clearly specify purpose of data collection and data use practices

## CONTEXTUAL



Design details based on the needs of users of this environment

## CULTURALLY SITUATED



Account for the appropriate cultural values and norms

## 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

## BARRIERS



Allow users the ability to temporarily disconnect from the IoT system

## ADAPTATION



Enable users to adapt the IoT system to reflect their preferences

## FORESIGHT



Consider the impact of IoT system on users and/or society over time

## ACCESSIBLE



Provide access to resources (person or other) for help and/or questions

## EQUILIBRIUM



List the benefits and potential/ likely risks to find the right balance

## ACCOUNTABILITY



Create mechanisms to ensure compliance and addressing user concern