Up Close and Personal: Exploring User-preferred Image Schemas for Intuitive Privacy Awareness and Control

Conference or Workshop Item

Up Close & Personal: Exploring User-preferred Image Schemas for Intuitive Privacy Awareness and Control

ANONYMOUS, Anon

Effective end-user privacy management in everyday ubiquitous computing environments requires giving users complex, contextual information about potential privacy breaches and enabling management of these breaches in a timely, engaging and intuitive manner. In this paper, we propose using empirically grounded image schema-based metaphors to help design these interactions. Results from our exploratory user study (N=22) demonstrate end users' preferences for changes in physical attributes and spatial properties of objects for privacy awareness. For privacy control, end users prefer to exert force and create spatial movement. The study also explores user preferences for wearable vs. ambient form-factors for managing privacy and concludes that a hybrid solution would work for more users across more contexts. We thus provide a combination of form factor preferences, and a focused set of image schemas for designers to use when designing metaphor-based tangible privacy management tools.

CCS Concepts: • **Security and privacy → Usability in security and privacy**; • **Human-centered computing → Interaction techniques**; **Empirical studies in interaction design**.

Additional Key Words and Phrases: privacy management; image schema; privacy metaphors; tangible interactions; ubiquitous environments

ACM Reference Format:
Anonymous. 2018. Up Close & Personal: Exploring User-preferred Image Schemas for Intuitive Privacy Awareness and Control. In *Woodstock '18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY*. ACM, New York, NY, USA, 20 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

The proliferation of ubiquitous computing systems (UbiComp) has transformed our everyday spaces into cyber-physical-social environments such as smart homes and smart cities. The private territory of an individual now expands beyond their physical boundaries to include virtual (cyber) territory [32]. This has increased the possibilities of undesired access to an individuals' physical space and attention (disturbances), or their information (observations), anytime and anywhere, raising serious privacy concerns [32, 34]. The embedded nature of UbiComp makes it challenging for people to dynamically perceive and control such privacy threats in their everyday lives. This leads to a lack of awareness of possible privacy implications, resulting in inadequate protection practices.

To enable an individual to effectively manage their privacy in everyday UbiComp contexts, it is essential to raise their awareness appropriately and give them effective controls [7, 46]. The majority of existing end-user interfaces that support privacy awareness and control are GUI based, and due to inconsistencies with our interactions in the physical and social world, pose several usability challenges especially when managing privacy dynamically [24, 43]. They almost always demand full visual attention, irrespective of the users' ongoing activity and available attention.

The interactions may not be readily available, appropriately granular or easy to remember in a given context of the user. The task feels buried inside a screen-based general-purpose device, making the privacy management interaction experience physically interruptive, socially disruptive and time-consuming in everyday settings [14, 41]. For example, it is challenging for a user to interact with a GUI-based privacy interface to manage their privacy while jogging, driving a car, holding shopping bags, or when in a meeting, without disrupting their primary activity. This makes dynamic privacy management complex, cumbersome and non-engaging for the end-user.

Due to their potential to provide high levels of realism and sensorial stimulation, rich feedback, physicality and familiarity; tangible and embodied style interactions have been proposed to address such challenges in privacy management [43]. Such interactions could allow the provision of feedback for privacy awareness through visual cues, sound, haptics or smell, and enhance privacy control with direct haptic manipulation, spatial interactions or full body movements.

To meaningfully map tangible input actions to output representations and enhance naturalness and intuitiveness in interactions, several researchers have explored and advocated the use of Image Schema based metaphors as a conceptual design tool [3, 20, 23, 40]. Image schemas are the recurring dynamic patterns of sensory-motor experiences (or bodily interactions) that structure our understanding of the world [25, 33]. Their metaphorical extensions generate primary metaphors [21]. Such metaphors are fundamental units of knowledge shared across a large range of people and can be retrieved subconsciously from memory [20]. Beyond supporting intuitive interactions [19], primary metaphors also promise inclusive interactions making them independent from conscious cognitive abilities, technical experience and cultural interpretations [21].

To systematically extract user-preferred primary metaphors for privacy management, we need to first understand the underlying image schemas. The literature provides different sets of general and universal image schemas [20, 25, 33, 40]. After careful analysis, we select a subset of schemas that reasonably conform to the constructs of user-centered privacy. Using this set, we then conduct an elicitation study (N=22) to find the most preferred image schemas for privacy awareness and control in everyday UbiComp contexts. We present these contexts to the participants in the form of storyboards that are inspired from the accounts of real-life privacy violations from various stakeholders across in-home and out-of-home settings.

As a result, we contribute a set of user-preferred image schemas for privacy awareness and control. The designers of tangible privacy management can use these to extract primary metaphors that are rooted in empirically established image schemas for privacy management and meaningfully inform the mappings between tangible input actions to output representations. To inform the tangible form-factor, the study further explores user preferences for wearable vs ambient form-factors for managing privacy in such contexts.

2 BACKGROUND AND RELATED WORK

In a context-aware and inter-connected world of ubiquitous computing, private boundaries get extended by virtual boundaries and result in new and unexpected privacy implications. Users are frequently found to be unaware of the privacy risks involved in the use of their mobile applications [4, 38, 54], technological systems [28], or the environment [6] they are in. This results in inadequate protection practices leaving individuals mentally, physically, socially and financially vulnerable.

2.1 Privacy Awareness and Control

The need for privacy awareness and control for end-user privacy management, is well described in the literature [7, 32, 35, 46]. There are many facets to how people decide whether a particular kind of access to them or their information is a privacy breach or not. Based on a review of several user studies of privacy in location sharing (e.g. [12]), mobile devices (e.g. [4]), and smart environments (e.g. [45]), and supported with his own studies, Koenings argues that *who* (recipient and relationship with them), *what* (content), *when* (context), *how* (processed, collected, distributed) and *why* (purpose, benefits), are the influential factors that affect users' awareness and control of their privacy [32]. Users give high priority to "who", "what" and "why" aspects, and desire systems that could enable them to be aware of observers and disturbers and control them at the same time [32]. Hence, by privacy awareness we mean becoming aware of the overall access, that may include any or all of the three important dimensions of access to one-self or one's information (i.e. who, what and why).

Users prefer manual or direct control of their privacy to indirect context-based control by pre-selecting privacy preferences [32]. Privacy control does not only mean blocking the access in every context. It is a bi-directional input-output process of boundary regulation where people can have too little, optimal or too much privacy [1]. When inputs from others and outputs to others are at an acceptable level to an individual, the optimal level of privacy is achieved. To achieve this optimum, an individual can take a variety of actions. Burgoon et al. studied these actions through a survey of the privacy concerns and the restoration behaviours adopted by 444 adults and adolescents [11]. In addition to blocking and allowing access, they found negative arousal and confrontation as one of the common mechanisms that people adopt to control their privacy. With miniaturization and the easy availability of recording devices, people have now also started recording privacy breaches to analyse, share or present as evidence of intrusion [5]. Hence, privacy control is having the ability to regulate the access to one's physical-self or information by blocking, allowing, confronting or logging.

We seek to identify user preferred image schemas and associated metaphors for such aspects of privacy awareness and control.

2.2 Metaphors for Privacy Management

Metaphors are useful to understand a concept in a relatively complex domain (target domain) by relating it to a concept in a more familiar domain (source domain) [8, 33].

To improve intuitiveness, many privacy UI researchers have used metaphors as conceptualising tools to increase end-users' awareness and enable them to re-actively or proactively control information privacy. Schlegel et al. uses the metaphor of eyes to give an accurate and ambient sense of a user's digital information exposure [50]. Eyes appear and grow in size depending on the number of accesses granted for a user's location and the type of person (family or friend) making the access. Lederer et al. use faces as encapsulation of privacy preferences [36]. Users can control with whom, what and when digital information is shared by changing faces. Tarasewich et al. propose blinders that mimic sticky notes to physically hide parts of a larger document [53]. This software-based method uses black squares to hide information on mobile devices in a public setting. To support privacy preserving spontaneous interaction for ubiquitous devices in physical proximity, Ferscha et al. uses the metaphor of an aura [15]. A digital aura is the strength of the device signals such as Bluetooth radio. It is dense at the centre of the object and thins out towards its surroundings. When the device detects another in its aura, it starts exchanging profiles and interacts on matching interest. A user can use information shields or filters to actively restrict profile propagation or passively control the incoming information. Kapadia et al. uses the metaphor of physical walls, and proposes Virtual Walls that could enable users to control the privacy of their digital footprints (contextual information derived from raw sensor readings) [27]. Three levels of transparency (transparent, translucent, and opaque) are presented enabling users to create different disclosure levels for their information. Nguyen et al. propose a mirror metaphor, representing privacy information at three levels: glance (gives a small amount of information), look (gives more information), and interactive (gives the most amount of information) [46].

We make no comment regarding the efficacy of these designs. What is notable is that the choice of metaphor within the design is only based on the designers' choice without an understanding of users' contextual preferences for the metaphor. Furthermore, even though most metaphors used have roots in the physical world, the modalities of user interactions offered by these designs are confined to visual representations and touch interactions on a GUI, which are not as grounded in the physical world as the metaphors themselves.

To provide users with subtle, real-time privacy warnings and non-obtrusive, instinctive control capabilities, Mehta et al. propose tangible style on-body privacy management [44]. They present Privacy Band: a forearm wearable that raises the privacy awareness of its' user through discreet haptic vibrations (metaphorical 'privacy itch') at distinct locations of their forearm and prompt them to react (or control) their privacy in an intuitive and immediate manner through direct haptic manipulation (metaphorical 'privacy scratch') [44]. While the 'itch and scratch' metaphors are inherently instinctive, need no visual attention and relate to the innate reflexes of humans, they have also been picked as a designer's choice rather than being informed by users' preferences in the context of privacy management.

2.3 Our Approach

In order to design privacy management interactions that are direct, natural and intuitive, we argue that there is a need to first have a better understanding of users' preferences for privacy metaphors. To achieve this, we follow a user-centred approach and extract the most preferred underlying image schemas for privacy awareness and control in everyday UbiComp contexts.

The literature shows differences in conceptions and perceptions of privacy across different age-groups [31, 52], particularly in dealing with online privacy [26, 39]. Zeissig et al. find variables such as user characteristics, attitudes and behaviours to influence such differences [56]. Therefore, to also account for age-related differences in image schema (conceptual constructs) preferences for privacy management, we conduct the exploration with 12 younger (below 60 years of age) and 10 older (above 60 years of age) participants. We believe that the extracted image schemas would provide designers with an empirically grounded set, whose metaphorical extensions could meaningfully inform the design of tangible privacy management tools for the two age-groups. To the best of our knowledge, we are the first to explore this.

3 IMAGE SCHEMAS AND INTUITIVE INTERACTIONS

Interaction designers often use metaphors as a conceptual tool for designing such interactions. Conceptual metaphor theory posits the existence of image schemas and how their metaphorical extensions are very effective in structuring and communicating abstract concepts [25, 33]. Based on their empirical study (N=65) on physical-to-abstract mappings in gestural interactions, Hurtienne successfully demonstrates the usefulness of image schema based primary metaphors for UI design [21]. The inherent physicality, familiarity and embodiment offered by tangible user interfaces (TUIs) particularly facilitate subconscious application of various image schemas, providing opportunities to design metaphor-based intuitive and effective interactions [20, 23, 40].

3.1 Selecting Image Schemas for Privacy Domain

Hurtienne et al. [20] and Macaranas et al. [40] explore and present various groups of image schemas that can serve as source domains for a variety of metaphors in abstract domains, when designing for TUIs. After careful analysis, we

Categories	Image Schemas
ATTRIBUTES	Heavy-Light, Dark-Bright, Big-Small, Strong-Weak, Warm-Cold, Rough-Smooth, Clean-Dirty, Fast-Slow, Hard-soft, Good taste – Bad taste, Good smell – Bad smell
CONTAINMENT	In-Out, Full-Empty
FORCE	Attraction, Compulsion, Balance-Imbalance, Blockage, Counterforce, Diversion, Enablement, Momentum, Removal of restraint, Resistance
SPATIAL	Up-Down, Front-Back, Left-Right, Near-Far, Centre-Periphery, Straight path - Curved path, Circular or Rotate
IDENTITY	Face, Matching (colour, pattern or size)

Table 1. Image Schema Grouped by Categories of Similarity

selected a subset of schemas (see Table 1) that conform to the general concepts, and constructs of user-centred privacy management (i.e. privacy awareness and its control). The first author focused on finding appropriate schemas for the constructs and second author focused on schemas for the concepts. Fine-tuning of the selected schema sets (modifying or dropping irrelevant individual schemas within those sets) was done collaboratively with the rest of the authors based on their domain knowledge of design and privacy.

ATTRIBUTE, SPATIAL and FORCE are particularly relevant to awareness and control aspects of privacy management. CONTAINMENT and IDENTITY are relevant for the overall concept of privacy itself. In the subsequent paragraphs, we explain this relevance.

SPATIAL and ATTRIBUTE schemas have been used in the past for designing more direct and natural interactions [20, 22, 40]. Privacy has often been described in terms of personal space that creates an invisible separation between the self and others [1, 51]. For example, this is reflected by the division of interpersonal physical space into intimate, personal, social, and public space in Hall's foundational work on proxemics [17]. Due to such spatial constructs, metaphorical extensions of SPATIAL schemas can be useful in choosing what kind of physical movements in a TUI could increase users' awareness of a privacy breach in real time. The changed position of a TUI element could also reflect the privacy status at a later point of time. These can also help in understanding spatial movements that a user would like to perform intuitively and discreetly to control their privacy. Similarly, ATTRIBUTE schemas can help to come up with metaphors that associate changes in observations and disturbances to the user with changes in the properties of any particular surrounding object.

The FORCE schema is inherently dynamic in nature like the concept of privacy itself which is about dynamically regulating the balance between the desired and the actual levels of access [2]. It can help users to express their experience of interaction when managing privacy (e.g., feel compelled to manage privacy). It also covers schemas such as blockage, enablement and counterforce that are also among the general mechanisms for privacy control.

Privacy has also been described as territory [13, 18, 29, 37], boundary [47, 48, 55], or borders [34, 42] that individuals regulate to manage their privacy [1]. When an observer or disturber tries to cross the private barrier (territory, boundary or border) of an individual and access their physical self or information in an undesired manner (to the user), it causes a privacy violation. Also, as the area within an individual's private barrier grows, the number of potential observers and disturbers within that barrier increases, increasing the probability of privacy violations. As the CONTAINMENT schemas include the concept of a container with a boundary, an enclosed area with certain contents, and an excluded area; the schema is analogous to the privacy concept itself.

One of the many awareness factors that influence privacy related decisions (and hence privacy control) by an individual, is the identity of the observer or disturber (who). Choosing different social identities in different social situations is also one of the proactive mechanisms of regulating (or controlling) privacy [36]. Metaphorical extensions of IDENTITY schemas could thus be useful in intuitively raising awareness and/or enabling control.

Other image schemas proposed by Hurtienne et al. [20] and Macaranas et al. [40] under categories such as BASIC, BALANCE, MULTIPLICITY and PROCESS, were considered but not included in the study. BASIC, was implicit in our study design as we used two non-functional tangible objects as props (more details in section 4.2). BALANCE was already included as a schema under the FORCE category, and did not warrant inclusion as a separate category (as presented by Macaranas et al.). Schemas in the MULTIPLICITY category are process-oriented, with relevance to what an observer does once they breach a users' privacy. As our focus was on aspects prior to that, on the users' own awareness and control of 'who' is accessing, 'what' is being accessed and 'why' (as discussed in section 2.1), this category is not relevant. Finally, PROCESS is not commonly accepted as an image schema [16], and had no clear connection to privacy management.

4 STUDY METHODOLOGY

To understand end-user preferences for image schemas for privacy awareness and control across everyday UbiComp contexts, we conducted a lab-based exploratory study. Next, we describe the design of our study material, participant recruitment, data gathering and the analysis methodology.

4.1 Storyboards

In a user-centred design process, storyboards are an important tool to illustrate a scenario in chronological order using easy-to-understand language [30]. To visually communicate how privacy violations could originate and unfold in different UbiComp contexts, we designed eight storyboards (see Table 2). These are inspired from previous consultations with different stakeholders (privacy experts, ordinary users) of different age groups. All (except S6) are based on their real-life accounts of privacy violations experienced across the cyber-physical-social worlds that they inhabit. S6 is based on hypothetically futuristic technology.

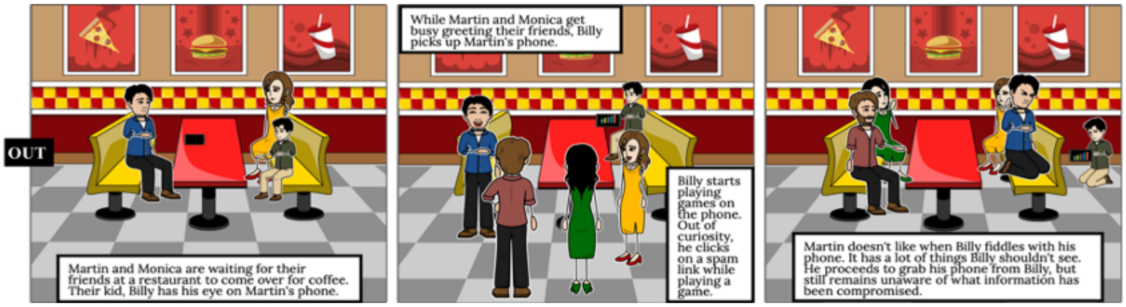
OUT
Martin and Monica are waiting for their friends at a restaurant to come over for coffee. Their kid, Billy has his eye on Martin's phone.
While Martin and Monica get busy greeting their friends, Billy picks up Martin's phone.
Billy starts playing games on the phone. Out of curiosity, he clicks on a spam link while playing a game.
Martin doesn't like when Billy fiddles with his phone. It has a lot of things Billy shouldn't see. He proceeds to grab his phone from Billy, but still remains unaware of what information has been compromised.

Fig. 1. S2: Physical access to a personal device by a family member, leading to leakage of sensitive information at a restaurant.

The storyboards visualise violations that involve undesired observations (S2, S3, S4), observations leading to disturbances or physical intimidation (S1, S5, S6). S7 depicts too much privacy leading to social isolation. S8 illustrates a proactive desire to manage digital privacy. S1, S3 and S7 are based in a personal space or inside-the-home settings

(IN). S2, S4 and S6 are based in public space or outside-the-home settings (OUT). S5 and S8 are applicable in inside-or-outside-the-home settings (IN-OUT). The storyboards also highlight a variety of contextual adversaries (observers and disturbers) such as company employees, family members, spam agents, acquaintances and drones. Along with the physical environment and adversaries, the central characters' main ongoing activity (and available mental and physical resources), also vary across the storyboards. In S7 and S8, the central characters' full attention is dedicated to proactively managing their privacy (no other sub-task involved). In S1-4 and S6, the central characters are busy with other activities and privacy management becomes more of an ad-hoc and reactive need. Due to space restrictions, we only illustrate one storyboard (S2) here (Figure 1). See [49] for the full set.

Storyboard Id	Description	Location
S1	Leakage of sensitive information, leading to physical access by cold callers.	Inside
S2	Physical access to a personal device by a family member, leading to leakage of sensitive information.	Outside (at a restaurant)
S3	Remote access to personal computer through social deception, leading to leakage of sensitive information.	Inside
S4	Physical access to a personal device by an acquaintance/friend, leading to leakage of sensitive information.	Outside (at a party)
S5	Leakage of sensitive information from mobile apps, leading to increased occurrences of disturbances through spam e-mails and posts.	Inside and outside
S6	Unexpected physical access by a delivery drone and announcement of sensitive information in front of friends, leading to embarrassment.	Outside (at the beach)
S7	Lack of social interaction, leading to too much privacy.	Inside
S8	Proactive management of access to personal information by mobile apps in personal device.	Inside and outside

Table 2. Storyboards details.

4.2 Non-functional "Magical" Devices

Props have been found to be useful for unfolding and exploring design possibilities when co-designing with the users [9]. Their openness, simplicity and hands-on-experience can help to evoke the future of artefacts in terms of shape, interaction, functionality, etc. [9].

To evoke physical-to-abstract mappings, we picked two non-functional tangible props: a cardboard cube box and a cloth sleeve (see Figure 2). The wearable sleeve (WS) provided participants with a form-factor for a wearable solution, while the ambient cube (AC) offered them a familiar object form-factor that would not have to be worn and could be kept around in a physical space. While WS was in the form of a sleeve, we encouraged participants to imagine it as a wearable for any part of the body as preferred and made up of any cloth that was felt to be comfortable.

These props were intended to be imagined as "magical" devices that could inform the participants about potential (or on-going) observations or disturbances, whenever, wherever they would desire, in whichever format they would be comfortable with. They could also interact with the devices in any way that its current form allows, imagining that any of their actions could be sensed. The devices were kept open-ended in terms of what they could do, as we did not want to restrict participant's choices by the perceived technical functionalities of the devices.

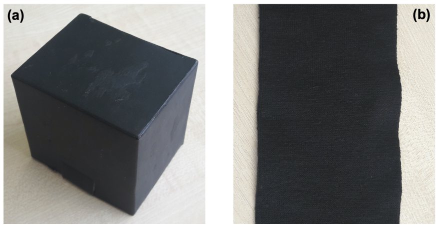

Fig. 2. (a) Ambient Cube (AC) (b) Wearable Sleeve (WS).

4.3 Questionnaire

Our questionnaire was divided into two sections with five questions each. The first section focused on privacy awareness. It asked about the participants' perception of awareness of the privacy dimensions (who, what, why) in a storyboard scenario, on a five-point Likert scale of importance. This part of the questionnaire was inspired by Koenings empirical work on understanding users' privacy concerns in ubiquitous environments like smart homes [32].

It also asked which out of the two magical devices the participant would prefer to use to raise their awareness within that particular scenario and how. Participants were first asked to express this for the overall violation situation and subsequently for the individual privacy dimensions (who, what, why), in terms of the image schemas under the categories of ATTRIBUTES, CONTAINMENT, FORCE, SPATIAL, and IDENTITY (see Table 1). These categories were provided to participants to choose image schemas from.

The second section focused on privacy control. It asked the same questions as in the first section, but for privacy control. The ATTRIBUTES schema was removed from the set of schema categories provided for control as it involved changes in the physical properties by application of some primary action, thereby making it a secondary level schema. We also deemed it more useful as a feedback schema rather than one for generating metaphors for control actions. The remaining four categories were provided to choose image schemas from. The questionnaire ended with an optional question to draw a solution storyboard for the given scenario, if the participant desired.

Individual questionnaires were created for each storyboard and the language customised to reflect the privacy violation within that storyboard.

4.4 Participants

Five pilots were conducted with people from mixed backgrounds. Three participants were below the age of 60 years (mean=39.7y, SD=11.6y). The remaining two participants were above 60 years of age (mean=74.5y, SD=14.8y). These pilots helped us refine the questionnaire language, adjust the interview approach and check the efficacy of the overall study.

Through convenience sampling, we recruited 22 participants as detailed in Table 3. A total of 12 younger participants (6 female) who were below 60 years of age (mean=34.4y, SD=5.9y) were grouped together and called Group Y (P1-P12). The remaining 10 older participants (6 female) who were above 60 years of age (mean=69.6y, SD=7.9y) were grouped together and called Group O (P13-P22). As in the pilot, we recruited participants from a mix of technical and non-technical backgrounds. We purposely selected participants from older and younger age ranges to develop a wider range of views across the population and look for age-related differences in the preferences for image schemas for privacy management, if any.

To scope the problem and remove confounding factors, participants were required to be fluent in English and not have severe cognitive impairments or dexterity issues.

Participant Id	Gender	Age	Occupation
P1	M	38	Researcher (computing)
P2	M	32	Software engineer
P3	F	29	Researcher (life-science)
P4	F	48	Secretary (computing)
P5	M	32	Software engineer
P6	M	28	Researcher (computing)
P7	M	40	Personal trainer
P8	F	29	Researcher (earth sciences)
P9	F	37	Software engineer
P10	F	29	Researcher (computing)
P11	M	37	Electronics engineer
P12	F	34	Cafe owner
P13	M	72	Retired (charted builder)
P14	F	82	Retired (univ-course manager)
P15	M	61	Lecturer (computing)
P16	M	62	Engineer
P17	F	77	Retired (magistrate)
P18	F	79	Retired (head teacher)
P19	F	61	Retired (head teacher)
P20	F	73	Retired (librarian)
P21	F	64	Retired (teacher)
P22	M	65	Handyman

Table 3. Participant details

4.5 Protocol

After receiving approval from our institution's ethics panel, we conducted semi-structured one-to-one sessions at our research facility or at the participant's home.

4.5.1 Step 1: Briefing and Priming.

Each session started with a short briefing about the study and participants were provided with printed copies of the information sheet. Participants were then asked to complete a consent form. A brief introduction was given on the concept of privacy, its violations, the need for awareness (who, why, what) and control (allow, block, confront, log), and challenges faced by individuals in mitigating privacy violations in everyday UbiComp contexts.

This was followed by an initial warm-up exercise (available at [49]) which introduced Image Schema concepts and provided participants with examples of metaphorical extensions of these schemas. Participants were presented with the selection of image schemas (see Table 1). To practice, for each schema category, participants were provided with a few incomplete sentences and asked to fill in the blanks and create simple primary metaphors: e.g., for ATTRIBUTES: Positive is _(bright)_, for FORCE: Work-life _(balance)_ is important for a healthy relationship.

Thereafter, two metaphor-inspiring pictorial representations (available at [49]) illustrating regulation of observations and disturbances in a public setting, were provided. Participants were asked about the underlying image schemas or metaphors in these pictures. This was to further contextualise the study and help them think in terms of primary metaphors for privacy management. Thereafter, the "magical" devices described earlier were introduced.

4.5.2 Step 2: Storyboards and Questionnaires.

Participants were presented with a pseudo-random selection of four storyboards, one after the other. This selection came from the set of eight storyboards [49] described previously. During the selection of four storyboards for each participant, we ensured that each set had at least one storyboard from IN and one from OUT, and that we achieved a balanced use of all eight storyboards across each participant group.

Once the participants read through a storyboard, they were presented with the questionnaire for that storyboard and asked to mark answers on the paper. Participants were encouraged to choose multiple image schemas and were helped if they required any further explanation. To assist participants' comprehension and thinking about image-schema inspired interactions, they were encouraged to think about 'who', 'what' and 'why' in terms of categories of 'who' (e.g., friends, family, strangers); 'what' (e.g., financial information, location, personal belongings); and 'why' (e.g., steal money, medical help). This process was followed for all of the remaining three storyboards. At the end of the session, participants were also given a chance to share any feedback. Overall, each storyboard was seen by 11 participants (6 from Group Y and 5 from Group O).

Throughout, participants were encouraged to think-aloud to help the researcher understand their underlying mental models. They were also reminded that the "magical" devices could behave however the participant imagined, as and when needed. The sessions were video and audio recorded, and notes were taken. Each session took 120 minutes on average. As a reward, participants were given a chocolate box or a plant worth approximately $6.

4.6 Analysis

The session recordings were transcribed. These were coupled with participants' written answers in individual questionnaire sheets and notes taken by the interviewer. Likert-scale data on perceived importance of privacy dimensions for awareness and control were aggregated across all the storyboards. Chosen image schemas and devices for privacy awareness and control across the storyboards were analysed, and the most preferred were established by counting the preferences of all the participants. Similarly, the most preferred image schemas for the awareness and control of privacy dimensions ('who', 'what' and 'why') were extracted. Further differences in preferences of image schemas based on participants' age group were also explored. For deeper qualitative analysis, inductive thematic analysis [10] was undertaken to establish common themes.

Given the exploratory nature of our work, a detailed statistical analysis of the differences between storyboards and participants was out of scope. This was because the large range of schemas, and the relatively low number of participants, made it impractical to undertake an exhaustive statistical analysis. Hence, throughout the results section, while we highlight some differences in the choice of schemas based on storyboards and age-groups, we do not claim any statistical validity for these differences and encourage further work to continue exploring these differences in future empirical investigations.

5 RESULTS

In total, 880 questions (4 questionnaires x 10 questions x 22 participant views) were answered by participants.

Our participants overwhelmingly found it important or very important to be aware of the 'who' (98%), 'what' (99%) and 'why' (~91%), dimensions of privacy. Controlling 'who' (~94%), 'what' (100%) and 'why' (93%) were also found to be important or very important. This strong desire to be aware of and control access from observers and disturbers has also been observed in previous work [32].

5.1 Preferences for Form-factor

Participants chose "magical" devices based on their physical structure, the need for immediacy in privacy management in a given storyboard and the overall context of the scenario. Some participants (P2, 3, 5, 11, 13, 16, 22) seemed to enjoy the hands-on nature of the props and kept playing with them through most of the study, exhibiting different interactions. "... [it] feels like inventing something", said P11.

5.1.1 Preferred Form-factor for Privacy Awareness.

Some participants chose form-factors for privacy awareness, independent of any scenario shown. A few participants (P4, 5, 7, 13, 14, 18) always preferred WS for the purpose of awareness, while one other participant (P20) always picked AC.

Overall, the wearable sleeve (WS) was generally preferred (~65%) across storyboards for awareness purposes, in particular for mobile and outdoor scenarios (~91% for S2, S4 and S6). Even indoors, WS was preferred when physical intimidation and disturbance was involved such as in S1 (~64%), where it was important to "feel the sensation urgently" (P12). Participants described the WS style device to be like a "part of body" (P4,6), which is "personalized" (P6, 9) due to closeness with body, "all-time available" (P2, 3, 10, 13, 14, 15, 16), easy to carry around, "discreet" (P8, 15, 17, 21, 22), and "easy to wear even with different cognitive and physical abilities" (P2, 4, 8, 14). P1, 2, 12, 13 found WS as an appropriate medium to communicate "urgency" when needed. The ambient cube (AC) was considered "less portable" (P3, 5, 9, 17, 19, 22), "easy to forget" (P7, 9, 14), could be "accessible by others" (P15) and "impractical" (P15) in such scenarios (S2, S4, S6).

The AC, however, was preferred by some (~35%) across storyboards for awareness purposes, slightly more for non-mobile and indoor scenarios such as S3 (~65%), or when there were no urgency and possibilities of more fine-grained awareness such as in S5 and S8 (~55% for the two scenarios). Participants expressed that they found AC to be appropriate in such scenarios because it felt less intrusive, "not required to be worn all time" (P3), "good to keep at home" (P3,21), can be kept "near the desktop" (P10,19,22), and something to "reflect with" (P5,9). P20 termed it as "safe" as it was "close ended" as opposed to the WS through which "things could escape" as it was "open ended". WS was also considered as something that could "constantly annoy" (P11, 14) and hold unnecessarily "high compulsion" (P11) for such scenarios, thereby suggesting few being wary of information overload through awareness notifications.

Figure 3 illustrates comparisons in % preferences of form-factors for awareness, between the two groups. While Group Y preferred WS for overall privacy awareness, it appears that their preference was not solely based on the scenario location. Group O on the other hand, based their choices mainly on the location context and primarily chose AC for indoor (S1, S3, S7) and WS for outdoor scenarios (S2, S4 and S6). Further work is needed to better understand how other factors may affect the preference in form factor.

5.1.2 Preferred Form-factor for Privacy Control.

A few participants always preferred WS (P13, 14, 18), or AC (P1, 20) for control irrespective of the scenario shown. Overall, both the WS and AC were almost equally preferred for control, with WS being selected slightly more (~53%). Similar to privacy awareness, the WS was mainly preferred for scenarios demanding quick access to the device for ad-hoc or immediate mitigation such as in mobile and outdoor scenarios (~73% for S2, S4 and S6), or indoors when the violation involved physical intimidation (73% for S1). The reasons stated to pick (or not pick) a particular form-factor were

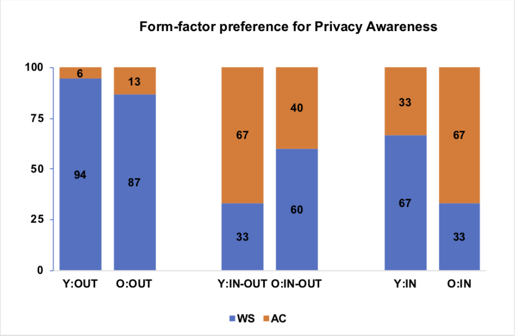

Fig. 3. Privacy AWARENESS: % times each form-factor was chosen for OUT (S2, S4, S6), IN (S1, S3, S7), and IN-OUT (S5, S8) scenarios by Group Y and O.

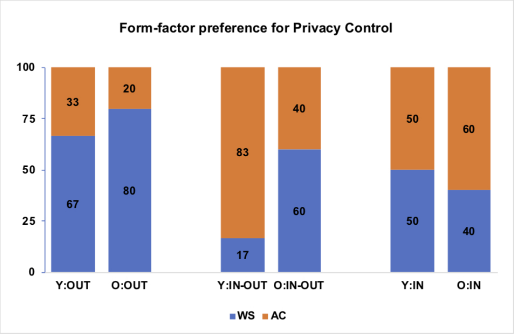

Fig. 4. Privacy CONTROL: % times each form-factor was chosen for OUT (S2, S4, S6), IN (S1, S3, S7), and IN-OUT (S5, S8) scenarios by Group Y and O.

similar to those quoted when choosing for awareness. For control however, the preference for AC was higher compared to that for awareness. This additional increase was probably due to greater possibilities of bi-manual interactions with AC having six different faces to work with and more "familiar" (P4, 10) and "playful" (P8) interactions. AC was also sometimes perceived to be "simpler and easier to understand" (P15) as well as something "physically stronger" and hence more appropriate for controlling as compared to WS which "felt softer" (P17).

Further, age-related comparisons can be seen in figure 4. The privacy control bar graph patterns for the two age groups vary in a manner similar to that of privacy awareness.

5.2 Image Schema Preferences for Privacy Awareness

When considering the scenarios, we encouraged participants to select as many schemas as they found appropriate. Their choices were rarely exclusive, with multiple image schemas being selected for each storyboard. Each of the 8 storyboards was seen 11 times (6 times by Group Y and 5 times by Group O), meaning that each image schema could be selected a maximum of 88 times (48 by Group Y plus 40 by Group O) for awareness. Therefore, the percentage data in Figure 5 illustrates how many times each schema category was selected by that group across all of the views of all storyboards by that group (e.g., 50% preference for a schema category by Group O would indicate that it was mentioned 20 times by them).

We did not find much difference in the choice of schema categories for privacy awareness across storyboards, meaning that the preferences did not vary much with the context. Overall for awareness, participants preferred image schemas from ATTRIBUTES (~78%), followed by SPATIAL (~69%). FORCE (~39%), CONTAINMENT (~22%) and IDENTITY (~24%) were chosen less often.

In Figure 7, we illustrate the % of times each schema was picked in the top two most preferred categories for privacy awareness, i.e. ATTRIBUTES and SPATIAL, by the two participant groups across all the storyboards. Please note that the image schema strong includes hard, and near-far includes centre-periphery because participants referred to them interchangeably. The rotate schema was perceived as haptic vibration. Also, smell refers to good and bad smell schemas. There was a difference in the number of schemas picked by the two groups in the SPATIAL category and hence different number of bars. The overall set of preferred schemas was however quite stable across the two age-groups, although some minor age-related differences in the individual schema preferences were seen.

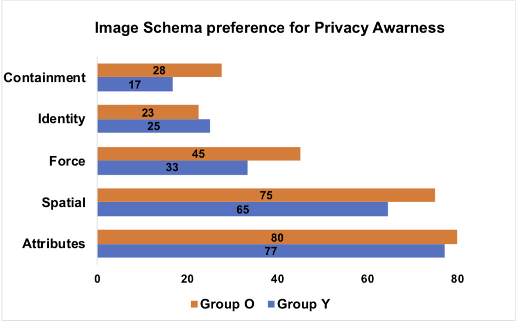

Fig. 5. Privacy AWARENESS: % times each image schema category was chosen by Group Y and O across all the storyboards.

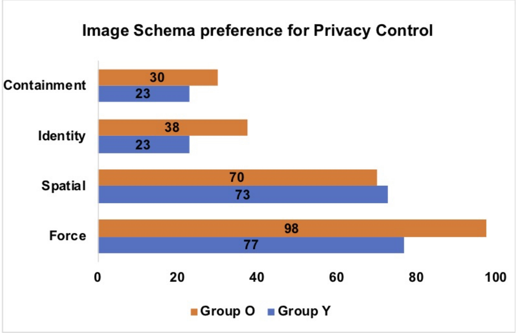

Fig. 6. Privacy CONTROL: % times each image schema category was chosen by Group Y and O across all the storyboards.

5.2.1 *Some Like it Hot.*

Several participants (16 out of 22) picked 'change in temperature' ATTRIBUTE as one of the preferred schemas for privacy awareness for one or more storyboards. To some, the warm schema was "like warning" (P1, 3-5, 9, 15, 17, 19) and was considered to represent "things that matter" (P15). P8 drew analogy from fiction quoting, "it [awareness] is like Harry Potter's coin, which becomes warm when something bad is going to happen". Some others referred the cold schema as "uncomfortable" (P6, 7, 11, 12, 14, 16-18, 22) and suitable for raising awareness about potential access. Even lack of access was equated to "lack of warmth" by few (P6, 14, 17, 19) suggesting it to express awareness about lack of social interaction.

5.2.2 *Gripping Stuff.*

Another set of ATTRIBUTES schemas that some participants found suitable for uncomfortable sensations and thus raise awareness, were rough (11 out of 22 participants) and strong (or hard) (13 out of 22 participants). These were chosen by the participants for one or more storyboards. "Rough is unpleasant, so hard to ignore", said P11. P19 drew analogy from fiction, "the warning could be like spikes on the back of the neck, like in Netflix series Stranger Things". A few specifically associated these schemas with access to location information (or physical self): "Strong grip is like physically someone is holding or accessing", said P4. "Rough on arm (or skin) is like physical intrusion into the house", said P7. P15 termed pinpoint location access "leading to pain sensation". P2 felt "[hard] tightening of the sleeve is like tightening your whereabouts".

5.2.3 *Bring it Closer.*

The near–far antonym pair was one of the most preferred SPATIAL schemas overall and was picked by 14 out of 22 participants for one or more storyboards. The majority considered the movement towards self or near schema like warning "…that someone is moving closer to me" (P4, 13, 14, 17, 22), "…someone approaching you physically" (P7, 15) and appropriate to "bring it [the potential issue] to forefront rather than burying inside" (P16). A minority (P6, 12, 19, 22) suggested the movement farther from self or far schema as a suitable representation of information going away or depicting social isolation (when friends and family felt socially far). The near-far pair was interchangeably referred to as centre-periphery, and so represents both pairs.

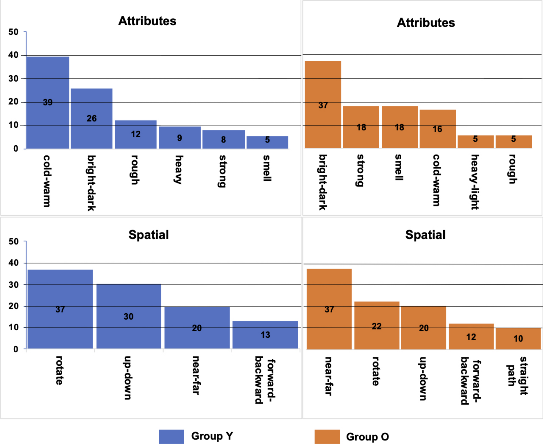

Fig. 7. Privacy AWARENESS: % times each Image Schema was picked in the top two most preferred categories by the two participant groups across all the storyboards.

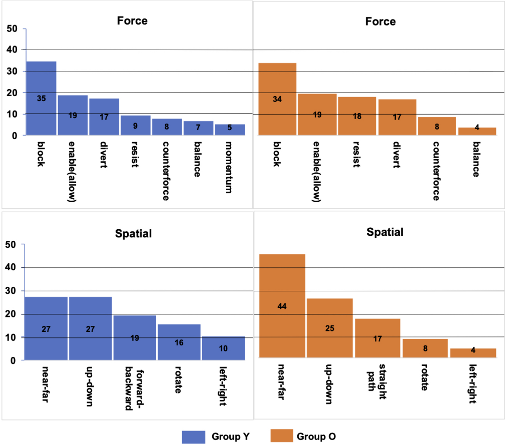

Fig. 8. Privacy CONTROL: % times each Image Schema was picked in the top two most preferred categories by the two participant groups across all the storyboards.

While the other schemas were chosen less often for general privacy awareness, they did give some interesting insights. For instance, FORCE schemas helped some participants to express the type of experience they desired in awareness interaction. The majority among them (group Y and O combined) desired the interaction to attract (~20%) their attention towards the imbalance (~18%) in their privacy and compel (~18%) them to resist (~19%).

IDENTITY image schemas were a natural choice for more fine-grained awareness across all the storyboards among both the groups. They found IDENTITY schemas suitable to refer to, for the awareness of ‘who’ (~88%) and sometimes (~47%) even ‘what’ privacy dimensions. For instance, out of all the IDENTITY schemas mentioned for the ‘who’ dimension, face or logo was the most preferred schema (~46%), followed by colour pattern like a traffic light system (~24%). Interestingly, text pattern (awareness through message) was hardly mentioned (~12%). Similar trends in the choice of IDENTITY schemas were seen when selecting for the ‘what’ dimension. The ‘why’ dimension was considered quite unrealistic or too descriptive to be informed through the available schemas by both the groups.

5.3 Image Schema Preferences for Privacy Control

Each of the 8 storyboards was seen 11 times, meaning that each image schema could be selected a maximum of 88 times for control. As explained in questionnaire design, we did not provide participants with ATTRIBUTE schemas for privacy control. They were encouraged to select as many schemas as appropriate from rest of the schema categories.

Overall for control, participants preferred image schemas from FORCE (~86%), followed by SPATIAL (~72%). IDENTITY (~30%) and CONTAINMENT (~26%) were chosen less often. The preferences did not vary much across contexts. See Figure 6 for group-wise % preferences.

Figure 8 illustrates the % of times each schema was picked in the top two most preferred categories for privacy control, i.e. FORCE and SPATIAL, by the two participant groups across all the storyboards. Please note that image schema rotate includes rotate clockwise and anti-clockwise, and near-far includes centre-periphery as participants referred to them interchangeably. There was a difference in the number of schemas picked by the two groups in the FORCE category and hence the different number of bars. Like in privacy awareness, the overall set of preferred schemas was quite stable across the two age-groups, although some minor age-related differences in the individual schema preferences were seen.

5.3.1 Squeeze it, Shake it.

FORCE schemas widely helped participants express the intention of their control action. All the participants chose block or enable (allow) schemas for one or more storyboards. Divert schema (13 out of 22 participants) and resist (10 out of 22 participants) schema were other popular choices. Participants sometimes also explicitly expressed those intentions through different physical action modalities such as squeeze (P7, 9, 18, 19), shake (P3, 16), turn down (P2, 12), brush off (P16), hit (P11), or pull (P11). "Want to squeeze them out of my space. It gives me physical control and helps me release my tension/stress", described (P9). P11 expressed "pulling the string is like controlling". However due to limited data points no significant direct mappings could be derived between the intent and the action modality.

5.3.2 Up the hill or down the dale.

Participants also used SPATIAL schemas to execute control intentions (expressed through FORCE schemas). Several schema antonym pairs were used. For instance, when chosen, up, forwards and rotate clockwise were almost always picked for allowing the access, while down, backwards and rotate anti-clockwise to block the access. For the pair closer to self - farther from self, two underlying themes were clearly visible. Out of those who chose near-far schema pair, one set (14 out of 22 participants) chose nearer to self for allowing the access (and farther for blocking) as it made them feel like bringing the accessor closer to themselves or allowing only to people who are socially close. The antonym, farther from self, made them feel like they are pushing unwanted accessors away from themselves. The other set of participants felt that to protect or block access of something from adversaries is like moving it nearer to self. Moving something farther leads to reduced control or more accessibility to the public.

Participants found it difficult to choose particular image schemas for finer control over the 'who', 'what' and 'why' dimensions. They referred to same schemas (FORCE and SPATIAL) as they did for the overall control mechanism. Additionally, IDENTITY schemas were also preferred at times, to augment detailed proactive management (e.g., for setting up 'who' is allowed to access 'what' and for what purposes ('why')). In ~25% of cases participants chose not to express control for the three privacy dimensions in terms of image schemas.

6 DISCUSSION AND IMPLICATIONS

Active privacy management has many facets. Access to the physical self or personal information can occur across cyber, physical and social worlds, with cascading and unforeseeable implications. Users need to be made aware of any access in a timely and efficient manner while avoiding information overload. Some contexts necessitate coarse-grained awareness, others need fine-grained information on who is accessing, what is being accessed and why. Based on such awareness, an individual's context, and weighing the costs and benefits of the access, an individual can (if they want to) then decide on their control strategy (reactive and ad-hoc, proactive), to block, log, confront or allow the access.

In order to extract user-preferred primary metaphors for intuitive privacy management that accounts for such inter-related factors, we explored the underlying image schemas for privacy awareness and control through real-life inspired scenario storyboards. Our storyboards covered the complexities of everyday UbiComp environments and varied in terms of the types of privacy violations, accessors, location and central character's activity, overall manifestation, and the need for immediacy and granularity in awareness and control. Our tangible props helped participants to imagine desirable form-factors for a future privacy management device and choose image schemas to express interaction modalities and functionalities.

6.1 One-size Really Does Not Fit All

In general, participants preferred the Wearable Sleeve (WS) ~60% and the Ambient Cube (AC) for ~40% of time, for privacy awareness and control across all the storyboards. However, their choices varied depending upon the context location and the perceived need of immediacy and granularity in management for that context. Designers could follow a generalised approach and design a wearable device suitable for some people, in some contexts. However, we argue that the range of preferences lends itself to more customised devices with different form factors for different contexts and age groups (see Table 4). While we acknowledge other design approaches could be effective, and encourage further work to explore those approaches, such a hybrid approach has a number of advantages.

To improve the interaction experience in privacy management, a hybrid approach, using both wearable and ambient form factors, could support a larger range of users and contexts, without compromising the benefits of one form factor for the other. The hybrid should use a single software configuration across an adaptable physical form factor. The wearable nature could enhance hybrid's portability and availability to the user in multiple contexts. It could also offer instant coarse-grained management of mobile and urgent privacy violation scenarios in an ad-hoc and potentially eyes-free manner. The ambient form could help prevent information overload, by giving the user the choice of when to engage with it without having to wear it all the time. Blending into the background, the ambient form could also offer a more familiar and richer set of bi-manual interactions for fine-grained privacy management.

Scenarios	**P-Awareness**		**P-Control**	
	Y	**O**	**Y**	**O**
OUT	WS (~94%)	WS (~87%)	WS (~67%)	WS (~80%))
IN-OUT	AC (~67%)	WS (~60%)	AC (~83%)	WS (~60%)
IN	WS (~67%)	AC (~67%)	WS-AC (~50%)	AC (~60%)

Table 4. Privacy AWARENESS and CONTROL: form-factor choices for age groups Y and O.

6.2 Image Schema based Metaphors for Managing Privacy

Our initial set of image schemas enabled participants to compare between different categories before picking those of their choice. Our results empirically demonstrate end users' preferences for the ATTRIBUTE and SPATIAL schema categories for general and ad-hoc privacy awareness, and the IDENTITY category for finer grained awareness. Similarly, for overall privacy control, end users prefer the FORCE and SPATIAL schema categories and extend these to include the IDENTITY category for proactive and detailed control. We further present the preferred set of schemas in these top categories to reduce the design space that designers need to consider when designing for image schema-based privacy awareness and control.

These schemas can be used to generate primary metaphors for privacy management (e.g., Warm/Cold IS Privacy Awareness, Near/Far IS Privacy Control). These metaphors could then enable end-users to effectively understand a privacy violation situation in a complex space and what to do about it in a timely and intuitive manner. Based on intended interactions and functionalities, designers can map the primary metaphors to interaction modalities and generate tangible interactions for privacy management. For example, ATTRIBUTE and SPATIAL schema-based metaphors for privacy awareness can be directly implemented as visual, haptic, kinesthetics or olfactory interactions.

While metaphors based on physical attributes and spatial properties have been proposed as guidelines for designing TUIs for abstract domains [20, 30], our schema-based metaphors can be used to design similar interfaces but for end-user privacy management. It should also be noted that while our user preferred schemas are suitable for expressing the degrees of importance, granularity and urgency of violations based on users' priority, this needs to be further explored systematically when designing such interfaces. Antonym schema pairs could be used as a scale to provide customised and continuous regulation of access. e.g., a cold-warm scale could be used by a user to manage their privacy warnings. If they choose warm to represent privacy warning then higher the intensity of warmth, higher would be the degree of importance. Implementing other schema-based metaphors such as FORCE and SPATIAL as actions for privacy control, further require appropriate choices of modalities.

While some minor age-related differences in the individual schema preferences were visible, the overall preferred schema set was quite stable across the two age-groups. Further exploration within each reduced schema set in the context (e.g., to disambiguate the antonym schema pairs) could provide specific physical to abstract mappings and generate specific primary metaphors for privacy management.

7 LIMITATIONS

We introduced participants to the general concepts of privacy and image schemas to develop a common understanding and structure the study; we acknowledge that this could have biased their responses.

While image schemas are powerful tools for generating conceptual metaphors for tangible interactions, they inherently posses certain limitations when it comes to generating a vocabulary for designing real-world user interfaces. Mutual dependencies and interrelationships between the schemas could cause potential disagreement between different analysts, and each could come up with a different set [19]. Fine-tuning such sets with empirical investigation is thus needed. In our empirical investigation, although we asked participants to choose their preferred schemas separately for overall privacy awareness and control, and then for their respective privacy dimensions, it should be noted that these were not mutually exclusive entities. Hence, it is likely that the chosen image schemas for one entity might have been applicable for other categories as well but were not added unless explicitly mentioned. It is also possible that while mentioning multiple image schemas for one entity, participants could have meant to have those in various combinations. Considering those combinations could have resulted in improved guidelines. However, we did not have clear data to explore that and so could only look at the image schemas independently.

We tried to cover the space of wearable and ambient devices through our non-functional props. However, participants were influenced by their knowledge of existing form factors and so we can't claim our results for all types of devices in wearable or ambient spaces. While we tried to cover the complexities of everyday UbiComp using a range of storyboards, it sometimes made the study overloaded and exhausting for the participants. A much smaller set would have been ideal. Storyboards also tend to lack the dynamic nature of real-time privacy violations and limits the embodied experience of such scenarios. This limits the extent to which we can claim the metaphors or corresponding interactions to be intuitive and preferred, when participants would actually face such scenarios in real-life. Future research could perform more in-context enquiries to explore specific form-factor designs and instinctive schema preferences.

8 CONCLUSIONS

This paper contributes findings from an exploratory study on image schemas for intuitive privacy awareness and control, across a variety of everyday UbiComp scenarios. We provide a focused set of user-preferred image schemas. The designers of tangible privacy management can use these to extract context specific primary metaphors for privacy management and meaningfully inform the mappings between tangible input actions to output representations. Based on our findings, we also argue that developing privacy management tools based on a single form factor is limiting, and that a hybrid solution would work for more users across more contexts. To determine such designs, we encourage designers to follow a user-centric approach involving designing multiple artefacts as per users' context and preferences, and evaluating them longitudinally in those contexts. In doing so, designers may start producing privacy management tools that provide users with greater awareness and seamless control over an increasingly complex set of privacy threats, thereby improving the overall effectiveness and experience of privacy management.

REFERENCES

[1] Irwin Altman. 1975. The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding. (1975).

[2] Irwin Altman. 1976. Privacy: A conceptual analysis. Environment and behavior 8, 1 (1976), 7–29.

[3] Alissa N. Antle, Greg Corness, and Allen Bevans. 2011. Springboard: Designing Image Schema Based Embodied Interaction for an Abstract Domain. In Whole Body Interaction, David England (Ed.). Springer London, London, 7–18. https://doi.org/10.1007/978-0-85729-433-3_2 Series Title: Human-Computer Interaction Series.

[4] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. 2013. Little brothers watching you: Raising awareness of data leaks on smartphones. In Proceedings of the Ninth Symposium on Usable Privacy and Security. ACM, 12. http://dl.acm.org/citation.cfm?id=2501616

[5] ayah bdeir. 2006. random search. http://ayahbdeir.com/work/random-search/

[6] R. Beckwith. 2003. Designing for ubiquity: the perception of privacy. IEEE Pervasive Computing 2, 2 (April 2003), 40–46. https://doi.org/10.1109/MPRV.2003.1203752

[7] Victoria Bellotti and Abigail Sellen. 1993. Design for Privacy in Ubiquitous Computing Environments. In Proceedings of the Third European Conference on Computer-Supported Cooperative Work 13–17 September 1993, Milan, Italy ECSCW '93, Giorgio de Michelis, Carla Simone, and Kjeld Schmidt (Eds.). Springer Netherlands, Dordrecht, 77–92. https://doi.org/10.1007/978-94-011-2094-4_6

[8] Max Black. 1955. Metaphor. Proceedings of the Aristotelian Society, New Series 5 (1955), 273–294. http://www.jstor.org/stable/4544549

[9] Eva Brandt and Camilla Grunnet. 2000. Evoking the future: Drama and props in user centered design. In Proceedings of Participatory Design Conference (PDC 2000). 11–20.

[10] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. Qualitative Research in Psychology 3, 2 (Jan. 2006), 77–101. https://doi.org/10.1191/1478088706qp063oa

[11] J. K. Burgoon, R. Parrott, B. A. Le Poire, D. L. Kelley, J. B. Walther, and D. Perry. 1989. Maintaining and Restoring Privacy through Communication in Different Types of Relationships. Journal of Social and Personal Relationships 6, 2 (May 1989), 131–158. https://doi.org/10.1177/026540758900600201

[12] Sunny Consolvo, Ian E Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. 2005. Location Disclosure to Social Relations: Why, When, & What People Want to Share. (2005), 10.

[13] Julian J. Edney and Michael A. Buda. 1976. Distinguishing territoriality and privacy: Two studies. Human Ecology 4, 4 (Oct. 1976), 283–296. https://doi.org/10.1007/BF01557915

[14] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: User attention, comprehension, and behavior. In Proceedings of the Eighth Symposium on Usable Privacy and Security. ACM, 3. http://dl.acm.org/citation.cfm?id=2335360

[15] Alois Ferscha, Manfred Hechinger, Rene Mayrhofer, Marcos dos Santos Rocha, Marquart Franz, and Roy Oberhauser. 2004. Digital aura. (2004). http://pervasive2004.soft.uni-linz.ac.at/Research/Publications/_Documents/DigitalAura-ferscha2004.pdf

[16] Joseph E Grady. 2005. Image schemas and perception: Refining a definition. From perception to meaning: Image schemas in cognitive linguistics 29 (2005), 35. Publisher: Berlin/New York: Mouton de Gruyter.

[17] Edward T. Hall, Ray L. Birdwhistell, Bernhard Bock, Paul Bohannan, A. Richard Diebold Jr, Marshall Durbin, Munro S. Edmonson, J. L. Fischer, Dell Hymes, Solon T. Kimball, and others. 1968. Proxemics. Current anthropology 9, 2/3 (1968), 83–108. http://www.journals.uchicago.edu/doi/abs/10.1086/200975

[18] Jean Hayter. 1981. Territoriality as a universal need 0. Journal of Advanced Nursing 6, 2 (1981), 79–85.

[19] Jörn Hurtienne. 2011. Image Schemas and Design for Intuitive Use. Ph.D. Dissertation. Technische Universitaet Berlin.

[20] Jörn Hurtienne and Johann Habakuk Israel. 2007. Image schemas and their metaphorical extensions: intuitive patterns for tangible interaction. ACM, 127–134.

[21] Jörn Hurtienne, Christian Stößel, Christine Sturm, Alexander Maus, Matthias Rötting, Patrick Langdon, and John Clarkson. 2010. Physical gestures for abstract concepts: Inclusive design with primary metaphors. Interacting with Computers 22, 6 (Nov. 2010), 475–484. https://doi.org/10.1016/j.intcom.2010.08.009

[22] Jörn Hurtienne, Christian Stößel, and Katharina Weber. 2009. Sad is Heavy and Happy is Light Population Stereotypes of Tangible Object Attributes. (2009), 8.

[23] Johann H. Israel, Jorn Hurtienne, Anna E. Pohlmeyer, Carsten Mohs, Martin C. Kindsmuller, and Anja Naumann. 2009. On intuitive use, physicality and tangible user interfaces. International Journal of Arts and Technology 2, 4 (2009), 348. https://doi.org/10.1504/IJART.2009.029240

[24] Lukasz Jedrzejczyk, Blaine A. Price, Arosha Bandara, and Bashar Nuseibeh. 2010. Privacy-shake: a haptic interface for managing privacy settings in mobile location sharing applications. In Proceedings of the 12th international conference on Human computer interaction with mobile devices and services. ACM, 411–412. http://dl.acm.org/citation.cfm?id=1851690

[25] Mark Johnson. 2013. The body in the mind: The bodily basis of meaning, imagination, and reason. University of Chicago Press.

[26] Alena Fiona Kaiser. 2016. Privacy and security perceptions between different age groups while searching online. B.S. thesis. University of Twente.

[27] Apu Kapadia, Tristan Henderson, Jeffrey J. Fielding, and David Kotz. 2007. Virtual walls: Protecting digital privacy in pervasive environments. In International Conference on Pervasive Computing. Springer, 162–179. http://link.springer.com/10.1007/978-3-540-72037-9_10

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

[29] B Konings and F Schaub. 2011. Territorial privacy in ubiquitous computing. In Wireless On-Demand Network Systems and Services (WONS), 2011 Eighth International Conference on, pp. 104-108. IEEE, 104–108. https://doi.org/10.1109/WONS.2011.5720177

[30] Rachel Krause. 2018. NN/g Nielsen Norman Group. https://www.nngroup.com/articles/storyboards-visualize-ideas/

[31] Michelle Kwasny, Kelly Caine, Wendy A. Rogers, and Arthur D. Fisk. 2008. Privacy and technology: folk definitions and perspectives. ACM Press, 3291. https://doi.org/10.1145/1358628.1358846

[32] Bastian Könings. 2015. User-centered awareness and control of privacy in Ubiquitous Computing. PhD diss. PhD diss., Universität Ulm.

[33] George Lakoff and Mark Johnson. 2003. Metaphors we live by. University of Chicago Press, Chicago.

[34] Marc Langheinrich. 2002. Privacy invasions in ubiquitous computing. In Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing. UbiComp. Citeseer. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.6.6743&rep=rep1&type=pdf

[35] Scott Lederer. 2003. Designing Disclosure: Interactive Personal privacy at the Dawn of ubiquitous computing. Unpublished Master of Science, University of California, Berkeley, Berkeley, CA. http://www. cs. berkeley. edu/projects/io/publications/privacy-lederer-msreport-1.01-no-appendicies. pdf (2003).

[36] Scott Lederer, Anind K Dey, and Jennifer Mankoff. 2002. A conceptual model and a metaphor of everyday privacy in ubiquitous computing environments. Computer Science Division, University of California.

[37] Jaakko T. Lehikoinen, Juha Lehikoinen, and Pertti Huuskonen. 2008. Understanding privacy regulation in ubicomp interactions. Personal and Ubiquitous Computing 12, 8 (Nov. 2008), 543–553. https://doi.org/10.1007/s00779-007-0163-2

[38] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. 2012. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. ACM, 501–510.

[39] Wiebke Maaß. 2011. The elderly and the Internet: How senior citizens deal with online privacy. In Privacy online. Springer, 235–249.

[40] Anna Macaranas, Alissa N. Antle, and Bernhard E. Riecke. 2012. Bridging the gap: attribute and spatial metaphors for tangible interface design. In Proceedings of the Sixth International Conference on Tangible, Embedded and Embodied Interaction - TEI '12. ACM Press, Kingston, Ontario, Canada, 161. https://doi.org/10.1145/2148131.2148166

[41] Paul P. Maglio and Christopher S. Campbell. 2000. Tradeoffs in displaying peripheral information. In Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '00. ACM Press, The Hague, The Netherlands, 241–248. https://doi.org/10.1145/332040.332438

[42] Gary T. Marx. 2001. Murky conceptual waters: The public and the private. Ethics and Information technology 3, 3 (2001), 157–169. http://link.springer.com/article/10.1023/A:1012456832336

[43] Vikram Mehta. 2019. Tangible Interactions for Privacy Management. In Proceedings of the Thirteenth International Conference on Tangible, Embedded, and Embodied Interaction. ACM, Tempe Arizona USA, 723–726. https://doi.org/10.1145/3294109.3302934

[44] Vikram Mehta, Arosha K. Bandara, Blaine A. Price, and Bashar Nuseibeh. 2016. Privacy Itch and Scratch: On Body Privacy Warnings and Controls. In Extended Abstracts on Human Factors in Computing Systems. ACM Press, 2417–2424. https://doi.org/10.1145/2851581.2892475

[45] Anne-Sophie Melenhorst, Arthur D Fisk, Elizabeth D Mynatt, and Wendy A Rogers. 2004. Potential intrusiveness of aware home technology: Perceptions of older adults. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Vol. 48. SAGE Publications Sage CA: Los Angeles, CA, 266–270.

[46] David H Nguyen and Elizabeth D Mynatt. 2002. Privacy mirrors: understanding and shaping socio-technical ubiquitous computing systems. Technical Report. Georgia Institute of Technology.

[47] Leysia Palen and Paul Dourish. 2003. Unpacking" privacy" for a networked world. In Proceedings of the SIGCHI conference on Human factors in computing systems. 129–136.

[48] Sandra Petronio. 2002. Boundaries of privacy: Dialectics of disclosure. Suny Press.

[49] Author Redacted. 2019. Study Repository. https://github.com/PrivacyMetaphors/Study

[50] Roman Schlegel, Apu Kapadia, and Adam J. Lee. 2011. Eyeing your exposure: quantifying and controlling information sharing for improved privacy. ACM Press, 1. https://doi.org/10.1145/2078827.2078846

[51] Robert Sommer. 1969. Personal Space. The Behavioral Basis of Design. (1969).

[52] Wouter M. P. Steijn and Anton Vedder. 2015. Privacy under Construction: A Developmental Perspective on Privacy Perception. Science, Technology, & Human Values 40, 4 (July 2015), 615–637. https://doi.org/10.1177/0162243915571167

[53] Peter Tarasewich, Jun Gong, and Richard Conlan. 2006. Protecting private data in public. In CHI'06 Extended Abstracts on Human Factors in Computing Systems. ACM, 1409–1414. http://dl.acm.org/citation.cfm?id=1125711

[54] Christopher Thompson, Maritza Johnson, Serge Egelman, David Wagner, and Jennifer King. 2013. When it's better to ask forgiveness than get permission: attribution mechanisms for smartphone resources. In Proceedings of the Ninth Symposium on Usable Privacy and Security. 1–14.

[55] Pamela Wisniewski, Heather Lipford, and David Wilson. 2012. Fighting for my space: coping mechanisms for sns boundary regulation. ACM Press, 609. https://doi.org/10.1145/2207676.2207761

[56] Eva-Maria Zeissig, Chantal Lidynia, Luisa Vervier, Andera Gadeib, and Martina Ziefle. 2017. Online Privacy Perceptions of Older Adults. In Human Aspects of IT for the Aged Population. Applications, Services and Contexts, Jia Zhou and Gavriel Salvendy (Eds.). Vol. 10298. Springer International Publishing, Cham, 181–200. https://doi.org/10.1007/978-3-319-58536-9_16