Privacy Care: A Tangible Interaction Framework for Privacy Management

Vikram Mehta
Computing and Communications, The Open University, Milton Keynes, UK, vikram.mehta@open.ac.uk

Daniel Gooch
Computing and Communications, The Open University, Milton Keynes, UK, daniel.gooch@open.ac.uk

Arosha Bandara
Computing and Communications, The Open University, Milton Keynes, UK, arosha.bandara@open.ac.uk

Blaine Price
Computing and Communications, The Open University, Milton Keynes, UK, b.a.price@open.ac.uk

Bashar Nuseibeh
Computing and Communications, The Open University, Milton Keynes, UK, bashar.nuseibeh@open.ac.uk
& Lero, University of Limerick, Ireland.

ABSTRACT

The emergence of ubiquitous computing (UbiComp) environments has increased the risk of undesired access to individuals' physical space or their information, anytime and anywhere, raising potentially serious privacy concerns. Individuals lack awareness and control of the vulnerabilities in everyday contexts, and need support and care in regulating disclosures to their physical and digital selves. Existing GUI-based solutions, however, often feel physically interruptive, socially disruptive, time consuming and cumbersome. To address such challenges, we investigate the user interaction experience and discuss the need for more tangible and embodied interactions for effective and seamless natural privacy management in everyday UbiComp settings. We propose the Privacy Care interaction framework that is rooted in the literature of privacy management and tangible computing. Keeping users at the centre, *Awareness* and *Control* are established as the core parts of our framework. This is supported with three interrelated interaction tenets: *Direct*, *Ready-to-Hand* and *Contextual*. Direct refers to intuitiveness through metaphor usage. Ready-to-Hand supports granularity, non-intrusiveness and ad-hoc management, through periphery-to-centre style attention transitions. Contextual supports customisation through modularity and configurability. Together, they aim to provide experience of an embodied privacy care with varied interactions that are calming and yet actively empowering. The framework provides designers of such care with a basis to refer to, to generate effective tangible tools for privacy management in everyday settings.

Through five semi-structured focus groups, we explore the privacy challenges faced by a sample set of 15 older adults (aged 60+) across their cyber-physical-social spaces. The results show conformity to our framework, demonstrating the relevance of the facets of the framework to the design of privacy management tools in everyday UbiComp contexts.

CCS CONCEPTS

•Security and privacy~Human and societal aspects of security and privacy~Usability in security and privacy•Human-centered computing~Interaction design~Interaction design theory, concepts and paradigms

KEYWORDS

Ubiquitous Computing, Privacy Management, Privacy Care Framework, Tangibility for Privacy.

1 Introduction

The proliferation of ubiquitous computing systems in our everyday spaces has nurtured the growth of cyber-physical-social environments such as smart homes and smart cities. Such systems often rely on implicit input from the people it surrounds. Their aim is to improve human lives by technologically addressing daily life challenges and offer people benefits with minimum effort. The private territory of an individual now expands beyond their physical boundaries to include virtual (cyber) territory [48]. This enhances the possibilities of undesired direct or indirect access to an individuals' physical space, attention or their information, anytime and anywhere, raising serious privacy concerns [48,51]. Personal information can be sensed from users' physical actions by observers (human and technological entities), recorded and uploaded invisibly to the Internet without warning. The constant interaction with, and interruptions from disturbers (human and technological entities) around a user can have a detrimental effect on their social relationships and mental wellbeing. Such outgoing *observations* and incoming *disturbances* can be termed as privacy threats, which originate from the cyber, physical and social worlds that individuals inhabit. The invisibility of many UbiComp technologies, makes it challenging for people to dynamically perceive and control such privacy threats, leading to a lack of awareness of possible privacy implications and resulting in inadequate protection practices.

Researchers argue that to enable an individual to effectively manage their privacy in UbiComp environments, it is essential to raise their awareness and provide them with effective controls [9,48,52,65]. The majority of existing end-user interfaces that support privacy awareness and control, do not really focus on the users' contextual needs and desires of interaction in terms of its style, modality or mechanisms. These are predominantly GUI based and restrict privacy problem presentation and solution finding to a screen-based system. The classic multiple-window and menu-based mechanisms of GUIs are useful, but due to inconsistencies with our interactions in the physical and social world, pose several usability challenges especially when managing privacy dynamically [40]. Firstly, they require a user to remember the sequence and location (in the GUI) of jargon-filled commands. Secondly, they also need the user to almost always, fully focus their (visual) attention on privacy management interaction and treat it as the central task, irrespective of their available mental resources or contextual management needs. The supported alert mechanisms are abrupt or intrusive, and controls are non-discreet. The task essentially 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 [25,59]. This makes dynamic privacy management highly challenging and cumbersome for the end-user.

When users lack appropriate awareness and control against the vulnerabilities, the need for support and *care* rises. The notion of *Privacy Care* particularly focusses on designing novel interactions to make the experience of users in privacy management, more effective and seamlessly natural in everyday settings. In order to achieve this, we propose using more tangible and embodied style interactions [3,18,32,37], thereby allowing the provision of feedback for privacy awareness through visual cues, sound, haptics or smell and enhancing privacy control with direct haptic manipulation [32], spatial interactions or full body movements [32]. Peripheral tangible interactions in particular, can help to avoid information overload by enabling users to pull information from their environment as and when appropriate [20], and fluidly shift between the centre and the periphery of attention when relevant for, or desired by the user [3,4]. Unless urgent, the initial feedback to raise awareness can be provided in the periphery of users' attention using modalities that suit to their context and the available mental resources. The user can then perform *microinteractions* [57] or 'inexact and inattentive' [33] type actions for quick control. These could be combined with more elaborate, precise and focussed tangible interaction mechanisms to also provide users with opportunity to dwell more into the privacy management task as needed and obtain higher awareness and exert finer control.

Meaningful tangible representations and intuitive controls can enhance users' interest and engagement, as well as providing them with a greater sense of control over their personal privacy. Rooted in the literature of privacy management and tangible computing, we provide a framework for designing such Privacy Care. Keeping users at the centre, *Awareness* and *Control* are established as the core parts of our framework. These are inherent to any tangible interface and are equally essential for the user's sense of personal privacy. The core is supported with three interrelated tenets: *Direct*, *Ready-to-Hand* and *Contextual*. Direct offers intuitiveness through metaphor usage. Ready-to-Hand supports granularity, non-intrusiveness and ad-hocness, through periphery-to-centre-to-periphery style transitions. Contextual supports customisation

through modularity and configurability. Together, they promise to provide experience of an embodied privacy care with varied interactions that are calming and yet actively empowering. Some sample scenarios to demonstrate how Privacy Care principles could be applied in everyday context:

Scenario 1: Adam has come to a non-familiar city to attend a conference. During his morning jog, he is about to enter a street with lots of CCTV cameras. His *Privacy Care* wearable artefact starts beeping and glowing red to inform Adam about a possible encounter with such observers in his upcoming environment. The wearable also suggests that he changes his route by glowing a green arrow pointing to another street where he won't encounter such observers. As a result, Adam chooses to manage his privacy by physically changing his direction of jogging (spatial control). While coming back from work in the night, when Adam receives the same feedback from his wearable artefact, he instantaneously feels that it is right to be seen (for safety) and takes the street with CCTV cameras which is also well lit and crowded.

Scenario 2: Adam has a Privacy Care ambient device in the form of an artwork hanging in his living room. It monitors the privacy settings of all the smart devices and applications that Adam uses, and communicates his overall privacy status by 'tilting' its position. The higher the potential of an undesired access to his smart devices, the higher the artwork tilts. During a working week at home, Adam has been allowing several applications to access his smart devices without paying attention to what data will be accessed and when. In the periphery of his attention, he can recognise the increasing tilt of the artwork, but due to his busy schedule, he is not able to attend to it. At the end of the week, when he is less busy, he walks to the artwork, gets curiously engaged, and starts focused interactions with different segments of the artwork to know what is actually going on and what controls could be executed. To access coarse-grained information and control, Adam knows he can re-balance the artwork, thereby removing access to all new applications and restoring his privacy levels back to his standard configuration.

Designers of privacy management systems need to empathise with users, understand their typical privacy needs, interactional capabilities and then tailor the *care* for them. Our framework thus focuses on the user interaction experience of privacy management in everyday context and contributes to the broader research agenda of usable privacy and security. The exploratory nature of the framework provides conceptual guidance on a set of dimensions, that interaction designers should follow when designing for effective and seamlessly natural privacy management. The resulting design concepts could then guide software engineers on the functionalities to develop and assist hardware engineers to think about the form-factors and modalities that are desirable.

To support the choice of our framework elements, we also present results from five semi-structured focus groups studies with a sample of older adults aged 60 and above. Research indicates that older adults are one of the most vulnerable groups when it comes to their cyber privacy [13,14,78], who also have high privacy concerns [61,93]. The effects of age-related decline in physical and cognitive abilities, alongside social factors can expose them further [75], making many (especially those living alone and technically inexperienced) an attractive target for privacy attacks in cyber, physical and social worlds they inhabit. Hence, we think that such a user group are one of the most important beneficiaries of the Privacy Care system. Once the designers understand the unique challenges of a specific population, they can improve technology for both the specific and the broader population [19].

Our study results conform to the framework principles showing their relevance to the design of privacy management tools in everyday UbiComp contexts.

2 Background and Problem Description

Privacy is an elusive concept. What is private to one might not be so private to others. On an everyday basis, individuals fluidly and intuitively refine their privacy choices. Altman describes privacy as a bi-directional input-output process of boundary regulation where individuals dynamically regulate access to themselves (or their information) based on internal changes in perception or knowledge, or external changes in the environment [2]. It is a non-monotonic function where people can have too little (e.g. crowding), optimal or too much privacy (e.g. social isolation) [2].

These core principles of Altman's privacy regulation theory are widely agreed upon and also extended by several researchers in the context of UbiComp environments such as [10,54,67]. For instance, Palen and Dourish extend Altman's social psychology theory to the networked, circumstantial world where

interpersonal interactions cease to be ephemeral and information can be easily recorded, made persistent and available to a wider unknown audience [67]. They describe privacy management as a continual, intuitive and dynamic response to a situation rather than static enforcement of rules which involves regulating boundaries of *disclosure* (private vs public life), *identity* (managing what to disclose about self and to whom) and *temporality* (past, present and future treatments of disclosed information) and the in-between tensions [67].

2.1 Privacy Management is Awareness and Control

Expanding the notion of privacy in UbiComp, Koenings explicitly defines awareness (and not only control) as a fundamental part of the right of privacy. In addition to an information-centric dimension, he also takes the user-centric physical dimension into account, and defines privacy management as an "*individual's right to be aware of potential observations and disturbances as well as an individual's right to control undesired observations and disturbances*" [48]. Observations or "*outgoing border crossings*" are "*the act of accessing personal information of a user*" by an observer [48]. Disturbances or "*incoming border crossings"* are *"the act of accessing a physical space or the attention of a user*" visually, acoustically or through motion by a disturber [48]. Observers are entities that gather contextual information in real-time and can be classified into *humans, ambient sensors, body sensors, personal device sensors,* and *personal device detectors*. These are present in the physical proximity of the user. Similarly, disturbers are entities that actively intervene in a user's physical territory and can be classified into *humans, ambient output devices, personal devices, autonomous devices,* and *remote controllable devices*. When an observer or disturber tries to cross the private (physical or virtual) boundary of a user and access them or their information in an undesired manner, it causes a violation of the user's privacy.

Besides the existence of an exponentially large number of possible situations of access in UbiComp; due to its' highly contextual, dynamic and personal nature, the notion of fully (and exclusively) automated privacy protection and control is not only inappropriate but also impossible. Researchers argue that to enable an individual to effectively manage their privacy in UbiComp environments it is essential to raise their awareness appropriately and provide them with effective controls [9,48,52,65]. Bellotti and Sellen argue *privacy as a user-interface design issue* and state four factors about which feedback and over which control should be provided to the user [9]. These factors are *capture* (when and what information about the user gets into the system), *construction* (what happens to the information), *accessibility* (who and what have access to what information), *purposes* (why information is needed and how can be used in the future) [9].

Nguyen and Mynatt propose the *Privacy Mirrors* framework to argue that in systems that encompass social, technical and physical environments, privacy is addressed best by giving users methods, mechanisms and interfaces to understand and then shape the system in all three environments and not just in any one environment alone [65]. Through their framework they suggest to provide: *history* of the information flow*, feedback* about history, flow and present status to raise *awareness* and provide *accountability,* and the ability to *change* in any of the three environments [65].

Rooted in a literature survey on several user studies under privacy in location sharing (e.g. [16]), mobile devices (e.g. [5]), and smart environments (e.g. [63]) 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 most influential factors that affect users' awareness. Users give high priority to "who", "what" and "why". They desire systems that could enable them to be aware of observers and disturbers, and directly control observations and disturbances originating from those entities at the same time [48]. He further argues that while social relationships are the most important factor while dealing with persons, trust and credibility are important when dealing with service providers. Based on these factors (or a subset), users decide whether an access to themselves or their information is acceptable or undesirable.

These frameworks essentially establish privacy management as an interactive task of receiving information about elements of access (raising awareness) and having the opportunities to control or regulate those elements (enabling control) in a continual and dynamic manner. Below, we discuss some of the approaches researchers have used when designing user interfaces to support the interactive task of privacy management.

2.2 Approaches for Designing Privacy Management Tools

While users need systems that enable them to be aware of potential violations and control them at the same time, it is also important to prevent an excess of information from overwhelming the user [15]. Managing the complex variety of privacy settings can make the task of privacy management cumbersome, time-consuming and uninviting. Hence, one of the biggest challenges of interactive privacy management in UbiComp environments is to provide the multidimensional information related to a potential privacy violation without overloading the user and enable intuitive control.

2.2.1 Coarse-to-fine Grained Management

To avoid overloading, many researchers support presenting information and enabling control at different levels from *coarse- to fine-grained* [48,52,65]. For raising awareness, Nguyen et al. urge designers to consider presenting feedback at different levels depending upon users' available attention, and how much are they willing to know and control in their present context [65]. They conceptualise this using the mirror metaphor where privacy information can be represented at three levels: *glance* (gives small amount of information like when a person walks by the mirror), *look* (gives more information like when someone stops and looks into the mirror), and *interactive* (gives most amount of information) [65]. Based on the information to present and users' context, designers are also advised to choose different *modalities* of presentation (and not only sight). Further, the *location* where to provide feedback also requires careful design [65]. When feedback is provided appropriately and in a timely manner, it could raise users' awareness, helping them to better understand their relationship with the cyber, physical and social environments which they inhabit. They could then take concrete steps to control their privacy by adjusting appropriately through available physical, social and technical means and address privacy concerns [65].

While fundamentally this approach is very useful for saving users from finding 'a needle in a haystack' every time they desire to manage privacy, it has been predominantly implemented with GUI style interactions in the past. Lederer presents a *Precision Dial* framework to intuitively enable users pre-configure or dynamically manage the disclosure of activity (or context) on-the-fly, but only to people who they know [52]. The user can control the disclosure precision across all dynamic information (but not static information) using a virtual dial and receive feedback through a log file [52].

Koenings presents the PriVis app with three views: *awareness view* (offers direct control capabilities for coarse-grained options), *privacy history view* (allows browsing of past implications), and *profile management view* (offers indirect control through pre-setting privacy policies for coarse and fine-grained options) [48]. The awareness and history view list all observation and disturbance channels in the user's territory (personal, physical and virtual-extended) in a tabular format. Information is presented at different granularity levels from coarse-to fine-grained [48].

We argue that for effective and seamless integration of dynamic privacy management in the daily lives of users, there is a need for coarse-to fine-grained mannerism in interaction style, modalities and mechanisms, and not just in information presentation. This is where existing work in this category fall short and needs attention.

2.2.2 Using Metaphors

Focussing on interaction and intuitiveness, many privacy UI researchers also propose the use of metaphors as conceptualizing tools to increase users' awareness and enable them to reactively or proactively control the information-centric aspect of privacy.

Lederer particularly focuses on the user experience in everyday privacy management in UbiComp. They present the *Faces interaction* framework, with three key abstractions: *inquirer*, *situation*, and *face* as an encapsulation of information precision preference [53]. It empowers users to present different fronts or social identities (what) to different people (who), under different circumstances (when) by allowing users to adjust the precision of personal information (*identity*, *location*, *activity*, identity of *nearby people* and *profile*) disclosure to *precise, approximate, vague* or *undisclosed* as desired [53]. However, the face metaphor is not found to be a suitable encapsulation for representing precision of dynamic information [52].

To give an accurate and ambient sense of a user's exposure to someone, Schlegel uses the metaphor of *eyes* [71]. 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.

To support privacy preserving spontaneous interaction for ubiquitous devices in physical proximity, Ferscha et al. [26] uses the metaphor of an *aura*. 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 surrounding. 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. [46], 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). Three levels of transparency (transparent, translucent, and opaque) are presented, enabling users to create different disclosure levels for their information.

We make no comment regarding the efficacy of such metaphor-based designs. What is notable is that the choice of metaphor within the design is mainly based on the designers' choice without an understanding of users' contextual preferences for the metaphor. Thus, it is not user centric. 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.

2.2.3 Overall Usability Challenges

The existing approaches to privacy management foreground understandability, reducing complexity and avoiding information overload. However, not only are they designed to operate in specific contexts, they also assume that privacy management must always be the main task (requiring full visual attention and some level of pre-planning), which makes it impractical for users to manage their privacy seamlessly and timely, in dynamic and contextually sensitive UbiComp environments.

Existing approaches also focus on screen-based solutions. The classic multiple-window and menu-based mechanisms of GUIs are useful, but due to inconsistencies with our interactions in the physical and social world, pose several usability challenges, especially when managing privacy dynamically [40]. There is a lack of immediacy in feedback and action. They demand full visual attention, irrespective of users' available attention or contextual interactional needs (in terms of its style, modality or mechanisms).

Overall, the privacy management experience becomes physically interruptive, socially disruptive and time-consuming in everyday settings [25,59]. The user is not able to push or pull the task of privacy management seamlessly between the periphery and the centre of their attention as relevant (context or desire). As a result, quite often users start postponing the management task or even lose interest in managing it at all. This makes them increasingly vulnerable to serious privacy violations in daily lives. As a result, we face three overlapping research challenges: RC1: To shorten the physical-digital interaction gap in active privacy management. RC2: To provide direct, intuitive and engaging interaction mechanisms for raising privacy awareness and enabling control. RC3: To enable ad-hoc transition between coarse-to fine-grained privacy management and its' seamless integration between everyday tasks without overloading and disrupting social and functional lives of the user.

To address such challenges and improve effectiveness, it is imperative to look at alternative interaction methods, modalities and mechanisms that are not only tailored to the privacy perceptions of individuals but also support seamless integration of privacy awareness and control between users' everyday tasks. In order to achieve this, we propose the notion of *Privacy Care* that involves using more tangible and embodied style interactions, thereby allowing the provision of feedback for privacy awareness through visual cues, sound, haptics or smell and enhancing privacy control with direct haptic manipulation [32], spatial interactions or full body movements [32]. Peripheral tangible interactions in particular, can help to avoid information overload by enabling users to pull information from their environment as and when appropriate [20], and fluidly shift between the centre and the periphery of attention when relevant for, or desired by the user [3,4]. In the next section we talk about such an approach, its relevance for dynamic privacy management and how it has been used so far in the context of end-user privacy management.

3 The Tangible Approach

The paradigm of tangible interactions is an alternative to GUI based approaches and provides methods, modalities and mechanisms to bridge the gaps between cyberspace and the physical environment. Nearly two decades ago Ishii and Ullmer proposed "tangible user interfaces" (TUIs) as interfaces that computationally

couple physical objects with digital information, enabling users to directly grasp and manipulate them (control) and perceive altered system states (representation) through human senses [37]. Tangible representations are often perceptually coupled with intangible representation (graphic and audio) [37]. There are two feedback loops: the passive haptic feedback loop (immediate confirmation that the user has grasped and moved the object) and the digital feedback loop (after sensing user's haptic manipulation, system changes its digital state and display results in visual or auditory form) [37]. Input and output spaces generally coincide to realize a seamless coupling of physical and digital worlds [37].

Hornecker and Burr expanded the concept of Tangible Interactions to cover a broader range of systems and interfaces that share "tangibility and materiality, physical embodiment of data, embodied interaction and bodily movement as an essential part of interaction, and embeddedness in real space" [32]. They identified four themes for designing and assessing tangible interactions in social scenarios: (a) Haptic Direct Manipulation, (b) Spatial Interaction, (c) Embodied Facilitation, and (d) Expressive Representation. *Haptic Direct Manipulation* refers to users' input (or control action) by physical (tangible) manipulation of material objects that are computationally coupled with digital information. *Spatial Interaction* focuses on the spatial qualities of an inhabited space where user interacts (or controls action) through meaningful movement and positioning of configurable materials (objects or her own body). *Embodied Facilitation* refers to how embodied constraints (such as size, form, or location of objects) in physical space and structure in software space can predetermine and guide style, methods and means of user interaction. *Expressive Representation* refers to perceptual coupling between tangible (such as haptic or smell) and dynamic intangible (such as graphics or audio) representations for providing meaningful output and raising awareness.

Tangible computing features provide possibilities for designing tangible user interfaces with explicit physical forms that are tailored for a particular application [36]. To understand which areas this interaction style can be suitably applied to, it is important to understand their inherent strengths and limitations. Shaer et al. provide an excellent review of the strengths and limitations of tangible computing systems [74]. TUIs can (1) support collaboration and shared discussions, (2) are physically and socially situated in the same world as we are, (3) facilitate tangible thinking and stimulation by leveraging natural connection of body and cognition, (4) enable space-multiplexed input that improves directness, integration and compatibility , (5) offer specific and expressive affordances by allowing designers to vary shapes, colours, weights, material and interactional constraints of the tangible objects, and (6) provide rich tactile or embodied feedback even supporting eyes-free control [74]. Such systems can often suffer with problems of scalability, physical clutter, bulkiness, lack of versatility, and user fatigue due to prime modality of interaction being physical at all times [74].

3.1 Seamless Everyday Interactions

Taking inspiration from how we naturally shift our attention and resources in everyday contexts from one central task to another, multi-task, and perform several activities in the periphery of our attention, several researchers particularly advocate peripheral tangible interactions for meaningful and seamless integration of interactive systems in people's everyday routine [3,4,20,30,66].

Building on Weiser's vision of "calm" technology [83], Edge and Blackwell propose "peripheral tangible interactions" that enable users to pull information from their environment "as and when appropriate, rather than information being pushed on to them by a range of technologies competing for their attention" [20]. The centre and periphery of attention are considered as dynamic states of the mind and not fixed categories of the world [20]. The focus is on designing tangible interactions that can engage both the centre and the periphery of a users' attention, enabling seamless back and forth movement between the two according to the momentary demands of a users' activity [20]. Such interactions are direct, imprecise but intentional, and episodic in nature.

Supporting calm technology, Bakker also advocates peripheral interactions that can fluidly shift between the periphery and the centre of users' attention when relevant for, or desired by the user [3]. They derive from the theories of divided attention which describe attention as finite amount of mental resources that can be divided over different activities such as bodily (e.g. sitting), cognitive (e.g. thinking) and sensorial (e.g. feeling the breeze) [45,85]. The extent to which these resources can be divided across multiple activities to be performed in parallel, depend on the type of resources required by those activities and their stage of

execution [4,85]. The activity that has the most resources allocated, is at the centre of attention, while all the other activities are at the periphery of attention [4]. The attentional process is also highly dynamic where the resource allocation across activities can constantly change, meaning seamless shifting of the activities between the centre and the periphery. Using three case studies, Bakker et al. demonstrate peripheral perception, interaction and combination of both the approaches [4]. The authors suggest perceptions and interactions should originate in the periphery where they become available to the user to enable easy and instantaneous initiation or even rejection [4]. The context of the interaction (users' location, social setting and their everyday routine) as well as personal preferences and differences, should also be taken into account for designing peripheral interactions [4].

Such interaction mechanisms hold high significance for the context of privacy management in UbiComp Environments, where a multitude of information pertaining to observations and disturbances needs to be represented and acted upon by a user, without overloading them or disrupting their ongoing activities in the social physical world. The coarse-grained information about a potential violation can be presented to the user in their periphery of attention unobtrusively and quickly attended to when urgent or desired, or ignored conveniently. It could also equally provide users with the opportunity to increase their focussed engagement with the stimuli, thereby pulling the privacy management task more and more to the centre, allowing them to perform more fine-grained interactions.

3.2 Tools for Privacy Management

There are few examples in the literature where concepts of tangibility (particularly immediacy and naturalness due to physicality) have been used to specifically help users regulate digital access to themselves in application contexts such as online social communications with known persons [21,29], setting mobile phone location [41], on-body data privacy warnings and controls [62], and securely unlocking a personal device [82].

Greenberg et al. [29] discuss and implement digital but physical surrogates (tangible representations of remote people) that indicate activity and availability of a remote person. Surrogates also react to a user's physical actions enabling natural ways of controlling digital communication. They also propose an awareness model and demonstrate the concepts of abstraction for balancing awareness, expressions, privacy and distraction during online interactions. This approach is limited to an indoor desktop context and helps to regulate disclosure in an online social interaction application with one-to-one intimate collaborators and not one-to-many or unknowns. Physical surrogates are explicitly visible to bystanders and thus could have privacy implications. No user evaluation is done to test whether it helps users to regulate their privacy or not.

Eggen et al. present IrisBox which uses continuous background sound to enable the user to be aware of their family or friends' availability and willingness to communicate [21]. Authors use the *metaphor of a door* which when closed, signifies keeping unwanted disturbances out, and when open, signifies openness and allowing access. The in-between states and positioning of the door also hold different interpretations and can add to the richness and subtility of the information. Through a continuous-input rotatory knob, the user can control access to themselves and set their own availability by physically twisting it on the IrisBox [21]. The outside world is represented with an illuminated background that becomes more and more visible as the user opens up the knob by rotating it anti-clockwise [21]. This also increases the sound output showing users' increasing availability [21]. Upon clockwise rotation, the illuminated background gradually shuts off, also turning off the sound output and representing no availability [21]. This approach is restricted to regulating availability/non-availability while communicating with a chosen few people. The system is meant to be used only indoors on a desk setting. This is also not evaluated with users.

Privacy-Shake [41] shows how haptic interfaces and interactions (shaking and sweeping) could help manage coarse-grained personal information privacy in an ad-hoc manner in mobile settings. In-lab evaluations with 16 participants shows that participants are able to perform the task of disabling location sharing faster with Privacy-Shake as compared with a traditional GUI. The task of shaking is found to be socially awkward and more discreet interaction is desired. Also, the functionality is highly limited and requires deeper exploration of interaction styles to regulate different aspects of regulating an access.

To provide users with subtle, real-time privacy warnings and non-obtrusive control capabilities, Mehta et al. propose on-body privacy management [62]. They present the Privacy Band prototype: a forearm wearable

that provides users with interactive capabilities to manage their cyber-physical privacy reactively in an ad-hoc, continuous and eyes free manner [62]. A lab-based user study with 11 participants has shown that it can help raise the privacy awareness of its' users 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') [62].

In the Touch-And-Guard system [82], Wang et al. address the problem of acoustic and visual eavesdropping while a user interacts with their personal device outdoors. The system uses hand touch as an intuitive means of establishing a secure connection between a wristband wearable and the touched digital device. It extracts secret bits from the hand resonant properties (highly sensitive to different hands, devices, and the manner in which hand touches the device) using accelerometer and vibration motors. These extracted bits are then shared by wristband wearable and the touched device to authenticate and communicate securely. The authors demonstrate the feasibility (and functionality) of their system through a lab-based study but do not test the user experience of privacy management.

Schaub et al. [70] vision an approach to use personal drones (such as Nanocopters) as interactive privacy interfaces in UbiComp environments, and discuss the opportunities and challenges. This approach represents a device-independent embodiment of information in user's physical environment. Information flow visualisation is represented through the flight path and swarming of the Nanocopters. For more information, the user can grab a Nanocopter and exert control, by interacting with its display, moving, or blocking its path or pushing it out of the path. These could also be used as ambient exposure displays or to facilitate in-situ privacy decision-making (for cases that need urgent intervention). The approach is not implemented. While this sets the vision, much is left to be explored. For instance, how to integrate such drones into smart environments without being obtrusive and threatening (to users as well as bystanders). It is also unclear how to design interfaces that can control the activity, representation and drone-user engagement.

3.3 Summary

Our literature review has highlighted the need to rethink how we design privacy management tools for UbiComp environments that individuals inhabit. GUI designs are overly complex, and do not respond well in the continually shifting context of such environments. We argue that TUIs provide many benefits for designing more effective privacy management tools, but as we have identified, existing proposals and designs have many limitations. We argue that there is a clear need for a unifying framework that can provide designers with a basis that is grounded in privacy and tangibility literature. Such a framework provides designers with a set of concepts that will help generate tangible interactions for effective and seamless privacy awareness and control in a variety of everyday UbiComp contexts. Building on our extensive review of the relevant, literatures, we present the *Privacy Care* framework.

4 Privacy Care: A Tangible Interaction framework for Seamless and Effective Privacy Management

The notion of *Privacy Care* particularly focusses on designing novel interactions to make the experience of users in privacy management, more effective and seamlessly natural in everyday settings. The framework is rooted in the literature of privacy management and tangible computing. Keeping users at the centre, *Awareness* and *Control* are established as the core parts of our framework. These are inherent to any tangible interface and are equally essential for the user's sense of personal privacy. The core is supported with three interrelated tenets: *Direct*, *Ready-to-Hand* and *Contextual*. Direct offers intuitiveness through metaphor usage. Ready-to-Hand supports granularity, non-intrusiveness and ad-hocness, through periphery-to-centre-to-periphery style attention transitions. Contextual supports customisation through modularity and configurability.

In the next subsections, we describe individual elements of the framework and how they can come together to provide experience of an embodied privacy care with contextually varied interactions that are seamlessly fluid, calming and yet actively empowering.

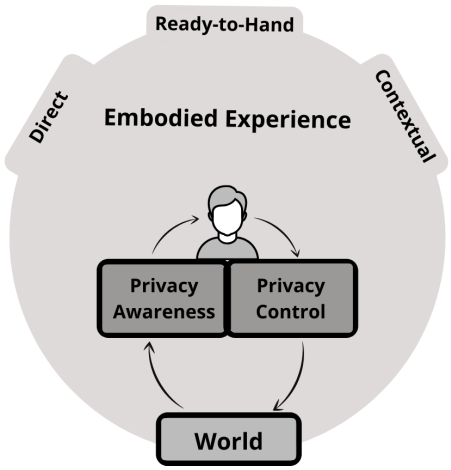

Figure1: The Privacy Care Framework

4.1 Privacy Awareness

Users are frequently found to be unaware of the privacy risks involved in the use of their mobile applications [5,56] and technological systems [47], or the environment [8] they are in. While users desire systems that can effectively improve awareness of privacy implications of their actions or inaction [48], it is difficult to determine what is sensitive for which individual, as different individuals can have different concerns and sharing tolerances in different situations [50]. These could also be influenced by age, gender and cultural perceptions of an individual.

Information Type

Effective privacy management first requires a user to be made aware of the relevant *aspects of access*, that could make it a potential violation having negative physical, mental or social implications. As highlighted earlier (section 2.1), Koenings argues that 'who', 'what', 'how' and 'why' are the key factors that impact on users' awareness. In a way, this covers all the aspects that a user can know about a situation or fact. The system should be able to deliver these (or their subset) appropriately as and when relevant to the user. For instance, in scenario 1 Adam only needs to know 'who' the disturbers are (CCTV cameras in the upcoming street). In scenario 2, Adam needs to know the 'overall status' and not just at a specific instance but any time as per desire.

One of the practical challenges that many users face while trying to manage privacy dynamically is to remember the sequence and location of control actions (that are usually jargon-filled in nature) in their devices. This becomes cognitively demanding and cumbersome. Hence there is a need to design for suitable cues that can inform a user explicitly about the available controls and provide more effective memory aids on how to execute them, especially in real-time. For instance, in scenario 2 the affordance of a titled (or imbalanced) frame is sufficient to inform Adam about the overall privacy health of his devices and action that he can perform to re-balance his privacy. This guidance could be very handy when there are multiple possible control actions and the user wants to choose one, or a subset of those in real-time. For instance, in scenario 1 Adam needs to be shown which could be a more privacy preserving route to take.

We add this aspect to the elements of Awareness, as illustrated in Figure 2 below.

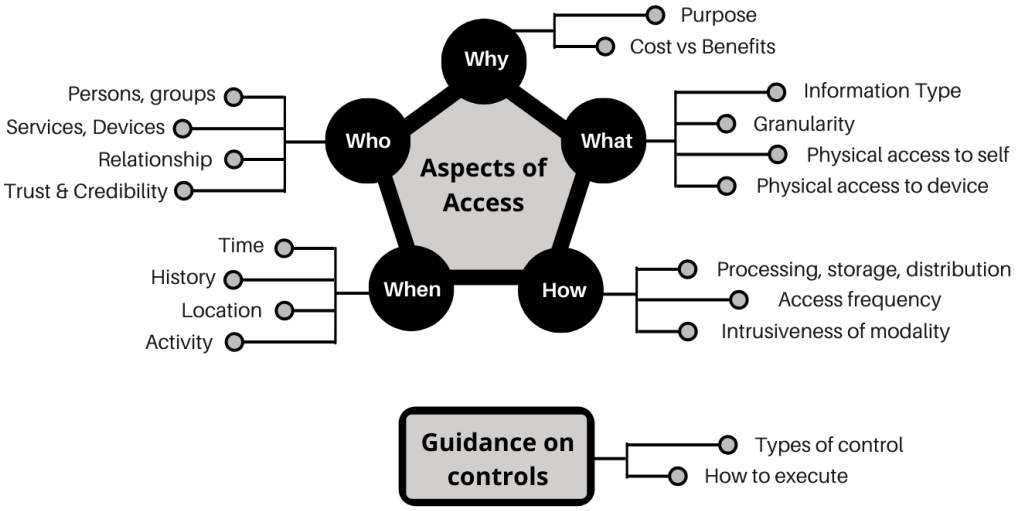

Figure 2: Information Types for Privacy Awareness

Interaction Style

The Privacy Care system can provide awareness information to the user through *prompts* or *reports*. While prompting can nudge the user to get aware of particular aspects of access and take appropriate control actions, reporting can provide information based on the consequences of users' actions. For instance, in scenario 1 Adam is prompted by the system to know about the upcoming disturbances and take a different route to control the access. In scenario 2, the artwork tilts to report the imbalance caused by Adam allowing non-trusted applications to access his devices.

Interaction Modality

Feedback can be provided to the user by changing physical properties, creating motion or projecting information on a Privacy Care TUI. The framework enables distribution of the multi-dimensional information types across different sensory channels through visual cues, sound, haptics or smell, as appropriate. The positioning of feedback input could be on the user's body or in the ambient environment around them. For instance, the forearm wearable Privacy Band informs the user of a potential violation through discreet haptic vibrations (metaphorical 'itch') on their body [62]. The appropriateness depends on the user's available attention and context. Thus, we advise designers to first empathise with users, understand their typical contextual privacy needs, interactional capabilities and then choose the right mix of tangible (and intangible) modalities for appropriate representation.

4.2 Privacy Control

Researchers have found users to prefer manual or direct control of their privacy to indirect context-based control by pre-selecting privacy preferences in the context of ubiquitous environments [48]. They desire systems that could enable them to control the overall access or the individual aspects of access (as described in Privacy Awareness).

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 on an acceptable level to an individual, the optimal level of privacy is achieved [1]. To achieve this optimal level, an individual can take a variety of actions. Burgoon et al. study these actions through a survey of 444 adults and adolescents about their privacy concerns and the restoration behaviours they adopt in interpersonal interactions [12]. In addition to blocking and allowing access, they find 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 it as an evidence of intrusion [7].

Control Types

Based on these views, we divide the control mechanism into three categories: *allow and block*, *confront,* and *record and report*. We propose using **allow and block** as the two ends of a dialectic scale where the optimal level of perceived privacy can be achieved anywhere on that scale. Such a scale could provide the user with an opportunity to decide upon and control the precision of disclosure dynamically as per their social, physical and mental context. The precision of disclosure can be like a four-step scale (as the one suggested by Lederer [53]), more fine-grained or even more coarse. **Confronting** the inquirer or adversary not only means negative arousal such as 'spamming the spammer', but also implies creating a socio-cultural situation of *you-know-that-I-know-that-you-know,* which is found to be effective in holding people accountable for their actions thereby improving their social behaviours [23]. Finally, through **record and report**, a user can either choose just to record but not report, report to their support network (e.g. friends, family) or to the authorities (e.g. council, police). See Figure 3 for illustration.

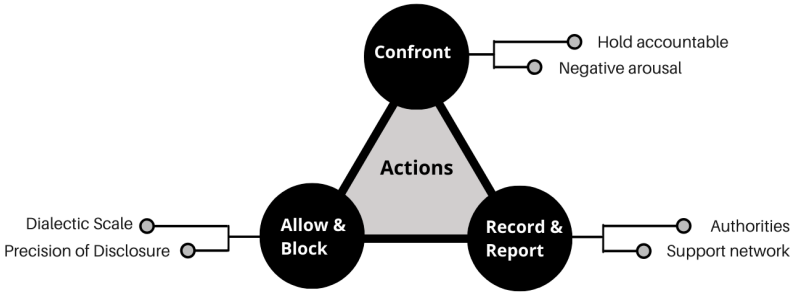

Figure 3: Control Types for Privacy Control

Control Style

Privacy Care systems can enable users to exert control actions *reactively* as well as *proactively*. Reaction is the immediate action taken by the user on receiving certain stimuli from the system. Pro-action is the action taken by the user pre-emptively based on their own understanding, without receiving any stimuli from the system. For instance, in scenario 1 Adam reacts to block access to his physical self. In scenario 2, Adam proactively allows applications to access his smart devices.

Designers should be careful not to fall into a 'notice and consent' style approach for every access as this could easily overwhelm the user very quickly. A fully automatic solution is also not possible or desirable as discussed in the related work (Section 2.1). Hence a semi-automatic approach such as the one proposed by Bunnig could be more appropriate, where a data-mining powered interaction model learns from a user's decision of which information to disclose to which service in which situation, and for any later point of time uses that to automatically decide or suggest for disclosure in that context [11]. This ad-hoc approach could save users from having to make frequent decisions [11]. The implementation manner is a system-level issue while our focus is on the user level. While out of scope for this paper, the concept needs to be explored in greater detail.

Interaction Modality

Privacy Care systems should go beyond touch interactions and support privacy control with direct haptic manipulation [32], spatial interactions or full body movements [32]. What direct manipulation [75] is to graphical user interfaces, tangible (haptic) manipulation is to tangible interfaces. This can involve meaningfully touching, tilting, pushing, grabbing, squeezing, shaking, scratching or rotating an object in the tangible interface. While direct manipulation requires visual attention and lacks naturalness of physicality, tangible manipulation when performed on the body for instance, can be done without visual attention by relying on proprioception and haptic feedback. For instance, Privacy Band offers a user the ability to restrict access to their information by physically manipulating (metaphorically 'scratching') a part of the band in an eyes-free manner [62]. Spatial interactions can feel even more natural and expressive. These focus on the spatial qualities of users' inhabited space, where the user can meaningfully move configurable objects or their own body in order to give input to the system. For instance, in scenario 1 Adam spatially interacts to regulate his privacy by changing the direction of his jogging. In scenario 2, nudged by the affordance of the

tilted artwork, Adam manages the access to his smart devices by naturally moving the artwork to a physically balanced position.

Different control interaction modalities can feel seamlessly intuitive and appropriate in different context. Again, we advise designers to first empathise with users, understand their typical contextual privacy needs, interactional capabilities and then choose the right set of control modalities.

4.3 Embodiment

The essence of Privacy Care lies in its' sensorial embodiment by integrating elements of privacy awareness and control into the everyday objects and environment around the user. As people are familiar with the forms and use patterns of such entities, augmentation only extends their existing capabilities, keeping the effort to learn as minimal. For privacy management that is seamlessly fluid, regular and yet non-interruptive, designers need to go beyond ordinary screen-based interactions that can sometimes feel buried inside a general-purpose device, and design meaningful interactions that are inspired not only from physical (tangible) but also social phenomena of daily life. Our aim with Privacy Care is to make basic privacy management interactions as natural and simple as a daily-life activity like 'drawing the curtain'. The tool to manage the task (the curtain in this case) is always tangibly present around the user in their particular environment but doesn't disturb or interrupt them in their ongoing tasks. The user doesn't even have to look or focus at it even while interacting (opening or closing) with it. The cue (or feedback for awareness) to draw the curtain either comes from the environment (e.g. when it is too bright) or from within (e.g. when a person wants privacy to change their clothes) in a very discreet and non-intrusive manner. The user then responds to cues such as the tool's affordance (grab and move in this case), using it to intuitively and naturally manage the privacy task, and return to their original task.

It is however also true that due to the multidimensionality of 'access' and the changing context in UbiComp environments, the privacy management task can't be that simple all the time. A user might sometimes need multiple and detailed bits of information to decide on whether a particular access would imbalance their privacy or not. A dedicated privacy management system based on Privacy Care should have the capability to rise up-to the demands of providing focused, detailed and more engaging interactions when relevant (as per the context or users' desire).

In any case, to achieve meaningful and expressive embodiment, it is necessary for Privacy Care to be appropriately direct, ready-at-hand and contextual throughout the daily routine of a user.

4.4 Direct

Privacy Care intends to offer interactions that enable a user to have direct access to their pre-existing knowledge and apply them intuitively to become aware of observations and disturbances in a quick, timely and a straight-forward manner. For an action and reaction based interactive system, in order to make interactions direct and intuitive, it is important to unify modality and other characteristics of action, i.e. time, location, direction, dynamics and expression, with the same characteristics of reaction [84]. However, full unification is not always possible when designing technical systems and so designers need to carefully design for information cues that can guide the user's actions towards intended functions [84]. Interaction designers often use metaphors as a conceptual tool for designing such interactions.

The directness and naturalness of tangible interactions is known to reduce cognitive load. The inherent physicality, familiarity and embodiment offered by tangible computing systems facilitate the subconscious application of prior knowledge, providing opportunities to design metaphor-based intuitive and effective interactions [38]. Hurtienne et al. propose a continuum of knowledge and describe that **intuitiveness** in interactions can stem from any level of that continuum: (1) *Innate,* (2) *Sensorimotor,* (3) *Culture,* (4) *Expertise* and (5) *Tools*, as long as they are unconsciously applied by the user [34]. As we move from the lowest level (Innate) to the highest level (Tools), the need for the degree of specialized knowledge increases and the potential number of users possessing that knowledge decreases [34]. For the context of Privacy Care, we stick to the first two levels which promises the most intuitive and universally applicable interactions.

Innate knowledge (e.g. sucking or grasping) are reflexes or instinctive behaviour which is acquired through the activation of genes or in prenatal stages of development [34]. The knowledge at sensorimotor level is

acquired in early childhood and used continuously in interactions with the physical world. Affordances [28] and image schema [43] reside at this level of knowledge [34]. While affordances are the cues for interaction offered by objects and environment around the user, image schemas are the recurring dynamic patterns of bodily interactions that structure our understanding of the world [43]. Image schemas are particularly useful as their metaphorical extensions generate primary metaphors which are very effective in structuring and communicating abstract concepts [34,43]. Such metaphors are fundamental units of knowledge shared across a large range of people and can be retrieved subconsciously from memory [34]. Beyond supporting intuitive interactions, primary metaphors also promise inclusive interactions, making them independent from conscious cognitive abilities, technical experience and cultural interpretations [35].

Innate metaphors such as 'itch' and 'scratch' have been used previously to alert users about personal data breaches intuitively, in a non-obtrusive and eyes-free manner [62]. In scenario 2, the nudge to balance the imbalanced artwork arises from the FORCE image schema, which enables Adam to make a metaphorical connection such that 'having balanced disclosure is balancing the artwork'.

Designers should continue to explore innate metaphors or the specific image-schema categories that are more suitable to the users in a given context for raising privacy related awareness and enabling control.

4.5 Ready-to-Hand

One of the biggest usability challenges with the existing solutions for privacy management is that they are not appropriately available to the user when needed. A lack of ad-hocness in interaction style, modality and mechanisms, result in either making the interaction too discreet and buried somewhere that it goes unnoticed, or too intrusive that it is right 'in the face' of the user. Overall, the task of dynamic privacy management becomes ineffective.

For seamless integration in the everyday lives of the user, we aim to provide Privacy Care that is ready-to-hand or ad-hoc but neither intrusive nor buried. To achieve this, in addition to context (as discussed in the next sub-section), it is important for designers to consider and then tailor the interactions for privacy management as per the availability of users' attention. Divided attention theory describes attention as the finite amount of mental resources that can be divided over different activities such as bodily (e.g. sitting), cognitive (e.g. thinking) and sensorial (e.g. feeling the breeze) [45,85]. The extent to which these resources can be divided across multiple activities to be performed in parallel, depend on the type of resources required by those activities and their stage of execution [4,85]. The activity that has most resources allocated, is at the centre of attention, while all the other activities are at the periphery of attention [4]. The attentional process is also highly dynamic where the resource allocation across activities can constantly change, meaning seamless shifting of the activities between the centre and the periphery [4].

4.5.1 Periphery-to-Centre Attention Transitions for Seamless Privacy Management

To design for periphery-to-center-to-periphery style transitioning of privacy interactions in a seamless manner, Privacy Care supports a **coarse-to fine-grained** style of presenting and enabling control over aspects of access, from existing privacy literature (section 2.2.1). It also expands the application of such mannerism to the interaction style and modality for privacy management.

The aspects of awareness and control can be presented in a coarse-to fine grained manner. For example, only 'what' is being accessed could be chosen by the system as the coarsest information to be presented and controlled by the user. It becomes less coarse when the next aspect such as 'who' is added, and so on. This is applicable to each individual aspect as well. For instance, 'who' can be made relatively coarse by enabling presentation and control through categorizing it into family, friends, colleagues and strangers or fine-grained by allowing to choose each and every person individually who can have the access and who cannot.

To be ready-at-hand, the Privacy Care system should be present around the user and easily accessible when needed in a context. This could be achieved by appropriately instrumenting everyday objects around the user or something that is portable and wearable for mobile situations like Privacy Band [62]. While the privacy literature mainly relies on a visual, text-based style for presenting aspects of access, and touch for control (whether coarse or fine grained), we advise the designer using Privacy Care to choose the presentation style and modality depending upon how coarse or fine grained the information and associated control is. For instance, presenting coarse information like 'what' is being accessed, can be more effective and less intrusive when presented on the body via haptic feedback [62]. Such feedback can reside at the extreme periphery of

users' attention. The user doesn't need to interrupt their ongoing task and can perceive the input in an eyes-free manner. Similarly, coarse interaction for control like haptic direct manipulation in an eyes-free manner [62], just shaking the phone [42] or even pressing on/off buttons, may be the only necessary control that a user desires or finds most instantaneous and effective when mobile or in a meeting. Minimum resources are needed to act and control such actions. As the granularity of information to be presented and control to be executed becomes finer, the richness of input and output modalities should also increase. Fine-grained privacy management requires the user to interact and thereby engage with the system longer. They generally demand deep focus and engagement to understand different aspects of a potential violation in detail and execute specialized control, thereby treating it as a task, central to the users' attention. For finer-grained management, awareness can be raised by distributing the access information across a combination of sensory channels. Properties such as intensity, frequency, duration can be manipulated. Similarly control actions can be provided as a combination of touch, haptic manipulation, spatial interaction or full body movement. To find the right combinations, designers are advised, to first empathise with users, understand their typical contextual privacy needs, interactional capabilities and then choose the appropriate set of feedback and control modalities.

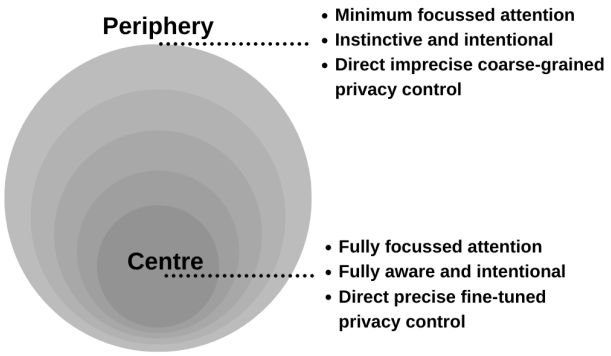

Figure 4: Coarse-to fine-grained privacy management interaction with a computing device on the attention continuum

Figure 4 illustrates the granular privacy management interaction on the attention continuum. Overall, the handle for privacy care should be provided to the user at their periphery of attention so that it is always available and ready to be dealt with when needed. The user can ignore it, perceive and spend minimum resources to act and control the access, or if curious, start pulling it towards the center of their attention by increasing focus and interaction, receiving higher feedback, and responding appropriately. They can start pushing it back away from the center anytime they desire, or when privacy has been managed sufficiently. For instance, in scenario 2, Adam first ignores the tilted artwork. As it is always present around Adam's environment, he interacts with it whenever he desires. The interaction also provides Adam, the opportunity to either coarsely balance the artwork with minimum attention and go back to his ongoing activity, or take time out and have more focused and detailed interaction with it.

The user's focus is then on the task in the context, rather than the artefact per se. This is in-line with Heidegger's notion of 'ready-to-hand' tools [31]. Sometimes, such as when the potential access is very critical, the system itself can push the privacy management task to the center of users' attention through stronger feedback, expecting the user to immediately push other ongoing tasks towards the periphery and make privacy management their central task. This kind of transitioning between the periphery-center-periphery, enabled through coarse-to fine-grained style, essentially enables seamless embedding of the task of managing privacy as a day-to-day activity.

4.6 Context

As seen in previous sections, to design for appropriate privacy awareness, control, intuitive metaphors and ready-to-hand interactions; understanding the user's context is very important. Contextual knowledge is what makes Privacy Care most effective and acceptable. It helps designers to precisely understand users' pain points, make effective design choices and set appropriate constraints. However, for building dynamically

interactive systems, gathering real and meaningful context information is not a trivial task even for modern day computing systems. Schmidt distinguishes context into *human factors* and the *physical environment* [72]. Human factors include static as well as dynamic information on the *user* (such as their habits, emotional state and biophysiological conditions), the user's *social environment* (such as information on others present around the user, social interaction and dynamics) and the user's *task* (such as activity, central task and peripheral tasks) [72]. The physical environment includes information on *location* (absolute and relative), *infrastructure* (points of observations and disturbances) and physical *conditions* (such as light, noise and weather) [72]. Having fully autonomous systems that can automatically detect the turbulent contexts and nuances of everyday activities and then act on the user's behalf is not only impractical but also seemingly impossible. Even if such systems become possible, they would take away all the control from its users and make them slaves of technology; a state that is not at all desirable to many.

4.6.1 Customizing for Context

Context has been found to affect users' interaction strategies and preferences in the usage of interaction modalities [55]. For privacy management, this complicates the situation further, as privacy is not a one-off task to be done in one context only. It is a dynamic response to a situation (and situations can change often in everyday context) rather than a static enforcement of rules [67]. To design for versatility, flexibility and extensibility, we propose the Privacy Care system to be customisable through configurable software and modular hardware. The aim should be to develop Privacy Care in a manner such that it can be presented as a kit that can be customised by the user themselves.

Modular Hardware

The physical elements of the Privacy Care system decide the overall form factor, user interaction style, input output modalities and associated metaphors for privacy awareness and control. The I/O elements could be designed as single independent physical entities and used as slave or extension modules to a main master module. For instance, Vonach et al. present such an approach and provide modular actuated tangible objects for tabletops [81]. Users can then arrange such modules in any specific layout picked from a finite set of layouts provided to them to craft their own socially meaningful interactional experiences. For example, when going to a meeting, a user can choose to assemble the Privacy Care TUI in the form of a wearable necklace with a 'heating' extension module as the actuator to provide feedback for awareness, and a 'touch' extension module as the sensor to provide action for immediate control. An underlining metaphor for privacy management interaction in such scenario could conceptualize access to users' real-time location by someone as *showing warmth* (by increasing temperature of the heating actuator).

Such customisation could be limited due to challenges of hardware design where a large number of I/O modules or layouts are possible.

Configurable Software

The underlying software is coupled with the physical elements of the system in a meaningful manner. Privacy Care system software should allow a basic configuration to initialize to default when set up for use. Basic configuration can manage the digital elements of awareness and control. Depending upon the selected I/O modules and the physical assembly, the software should re-configure to provide Privacy Care functionalities for desired interaction styles and modalities.

Software designers can divide feedback and control functions into two levels, (a) *secondary level*: provides feedback and control for a general type of violation which may not be time critical, and (b) *primary level*: provides feedback and control for something that is more specific to the context and needs immediate action. This distinction can help to avoid cognitive overloading and implement the Privacy Care system more effectively in a context. For instance, managing physical intrusion by public recording devices is of prime concern for Adam in scenario 1 and needs to be acted upon as and when it happens. This would be implemented at the primary level. When Adam goes on jogging every time, the sensing system gets activated to sense that particular form of incoming violation, inform Adam effectively and enable intuitive controls. Any other type of access that is not relevant to context, for example, someone tagging Adam on a social media post or a mobile phone application trying to access some data in his phone, would be implemented at the secondary level. These potential privacy violations would not be notified to Adam in that context unless he intentionally stops and wants to manage those.

To inform the design of the primary level, preferences can be collected from a user on what type of accesses they are most concerned with in different contexts. The remaining types of relevant potential violations can be put at the secondary level. The system can then change the functions for feedback and control at the primary and secondary levels, as the user's context changes.

Overall, Privacy Care focusses on personalising the interaction experience of privacy management based on the user's context. Designers are advised to follow a user-centric **research-through-design approach** [88]. This means that they must apply Privacy Care principles to empathise with and understand users' privacy management contexts in everyday routine, design artefacts, and evaluate them longitudinally back in those contexts, in an iterative manner.

5 User Study

We empirically support the choice of the elements of Privacy Care through five semi-structured focus groups with a sample set of older adults aged 60 and above. The focus groups explore the privacy concerns, mitigation approaches, and associated constraints faced by our user group in the context of daily life UbiComp contexts. Our methodology focuses on individual *lived and felt experience* and demonstrates how such an approach can be effectively used in the field of privacy studies [86].

We choose older adults because research indicates that they are one of the most vulnerable groups when it comes to their cyber privacy [13,14,76], who also have high privacy concerns [58,89]. While many IoT technologies are being designed to help older adults successfully and independently age in place, the ubiquity of such technologies also exposes them to serious privacy threats. The effects of age-related decline in physical and cognitive abilities, alongside social factors – including the loss of a spouse or close family/friends, the loss of income and loneliness [73] – can expose them further, making many (especially those living alone and technically inexperienced) an attractive target for privacy attacks.

5.1 Methodology

Focus groups enable group interaction and can provide greater insights into people's experiences and opinions [6,49]. They allow participants to selectively disclose, responding to others' comments as the conversation flows. Literature suggests focus groups as an appropriate research method to examine sensitive issues [1,2,3], as people may feel more relaxed when they see others describing similar experiences or views. Moreover, previous research has also established that semi-structured focus groups are effective for studying and understanding the needs of older adults [6], as they enjoy conversations where they can relate incidents and share stories of their own experiences. Based on this rationale, focus groups were considered appropriate to explore the sensitive topic of privacy with a sample of older adults.

Focusing on an individual's experience, as promoted by experience-centered design [86], has proven to be a useful and critical means of gathering information [60]. Such an approach helps in gathering users' "*affective and emotional response, the meaning that people make of interaction, people's values, the aesthetics of interaction, personal and social commitments to sustainability and democracy*" [60]. Dunphy et al. [19] followed an experience-centered approach to understand the privacy and security needs and practices of users. They used three case studies to co-design with users with methods including collage building, questionable concepts and digital portraits. These methods were tailored specifically to the participants and the settings involved. The researchers' motive was to learn from the participants' experiences. Through our exploratory study, we decided to utilize a similar method. We focused on a rich, grounded approach based around individual stories to explore already felt and lived experiences, motivations, concerns and interactions of the participants in the context of privacy in daily life settings.

5.2 Questionnaire

Our study was guided by individual questionnaires for each participant (see supplementary material [61]). The questionnaire (consisting of 22 questions) was divided into two parts. The first part (13 questions) aimed to map the daily routine of a participant to understand their information flows and any points of (physical and digital) interaction. Participants were asked to complete this part individually. The first part helped to set the context for a deeper discussion on privacy in the second part.

The second part started with a basic introduction to what we mean by privacy and how it can be violated in the physical and digital world (using pictorial representations). A 10-minute video excerpt from the movie "The Circle" [69], portraying the effects of unexpected privacy violations was also shown to the participants. This was followed by nine open and closed questions that explored the privacy concerns, awareness tendencies and mitigation approach currently followed by the respondent. It included a five-minute exercise in which we asked each participant to go to the privacy settings of their personal device and browser and turn on 'do not track' and delete 'cache and history'. Participants were asked to discuss the questions in this part collectively, building on each other's views and experiences while recording their answers individually.

5.3 Protocol

After receiving University ethics approval, we conducted two pilot studies to explore the efficacy of the questionnaire. This helped us improve the questions (e.g. modifying the language and presentation to make it more suitable to the local older adult population), methodology and overall structure of the study. Five focus groups were then conducted over a period of one year with three participants in each group. The groups were selected based on the availability of participants (first-come first-serve basis).

For every focus group, participants were asked before the study to bring their personal digital devices to the session. Each session started with a short briefing about the study and participants were provided with printed copies of the study information sheet. Participants were then asked to complete an informed consent form. Individual questionnaires (described earlier) were then given to the participants and the focus group was conducted. It was stressed that the term privacy is not only related to personal "data" but is also about the physical self; thus when a person crosses into an individuals' (physical or digital) territory, space or border against the individual's wishes, it is considered as a privacy violation.

As the study expected participants to share their private experiences, the consent form mandated that all the members of the group respect the confidentiality and privacy of others and to not share personal information with anyone outside the group during or after the study. With participants' permission, all of the sessions were video, and audio recorded. A moderator helped with note taking. Each study took an average of three hours, including a lunch break. Participants were free to leave the study at any time.

5.4 Participants

Our user group for this study were adults aged 60 and above. To scope the problem and remove confounding factors, participants could have age-related mild declines in sensory, perceptual, cognitive and communication abilities but were excluded if they had serious mobility conditions, motor disability, stroke history or cognitive impairment. All had some exposure to digital/internet usage.

With the help of Age UK (a UK based charity that works with and for older people) and local contacts, we recruited 15 participants (three males, mean age = 72.4y). All were British nationals. Six participants marked their living status as alone. While all were retired, five did not mention their background (see Table 1). It should be noted that we adopted a convenience sampling approach and do not claim the participants to be particularly representative of the older population.

Four focus groups were conducted at the university campus and one at a pub in the neighborhood of that particular group. Participants were served lunch as compensation.

5.5 Analysis

The session recordings were transcribed. These were coupled with participants' written answers in the individual questionnaire sheets and notes taken by the moderator. The data provided deep qualitative insights into the daily life circumstances of older adults in which privacy violations can occur, their approaches to mitigate privacy risks and regulate disclosure, and challenges encountered in the process. Deductive thematic analysis of the data was performed to categorize it into pre-determined categories, i.e. Privacy Awareness, Privacy Control and Interaction challenges viz, intuitiveness, granularity and customization to context. Factors such as frequency, uniqueness, and actual or possible degree of (mental or physical) harm to the older adults, were taken into consideration when picking data for supporting each of the category.

Group	ID	Age	Sex	Former occupation	Living Status
G1	P1	80	F	Course manager	Alone
	P2	77	F	Head teacher	Alone
	P3	71	M	HR professional	With partner
G2	P4	76	F	Magistrate	Alone, in apartments for older
	P5	70	M	Charted Builder	With partner
	P6	73	F	-	Shared house
G3	P7	84	F	Accounts worker	With partner
	P8	90	M	Auto foreman	With partner
	P9	60	F	Accounts admin	With partner and children
G4	P10	86	F	-	Alone
	P11	72	F	-	With tenants
	P12	63	F	-	With partner
G5	P13	60	F	Social worker	With a dog
	P14	65	F	Housing officer	With partner
	P15	60	F	-	Alone

Table 1: Participant details (N=15).

5.6 Results

Throughout the sessions, participants shared several personal stories of privacy violations that related not only to the cyber world but ranged across their cyber, physical and social lives. This helped us to understand their real contextual needs and challenges in managing privacy in everyday UbiComp situations. Below we describe the themes that were identified to represent the needs of privacy management for this set of participants.

5.6.1 Privacy Awareness

Like many previous usability studies in the privacy literature, our participants also showed a severe lack of privacy awareness. Most agreed that they could not often sense threats to their privacy in real-time. In the physical world, only 3 (of 15) participants felt they could usually sense this risk with the remaining reporting 'sometimes' (n=7), 'rarely' (n=4) or 'never' (n=1). For instance, participants had concerns about shoulder surfing into their personal device by anyone around them, anytime without their knowledge, especially when using online banking services in public places (P1, P4-6). Some (P2, 10, 13-15) felt physically vulnerable while interacting with cyber-physical devices such as ATM machines in open spaces, especially at night. "*Somebody came over the top of me and tried to take my card. He didn't get my card but he sort of entered into my personal space and leaned over me. I didn't even see that it was going to happen*", said P13.

For the digital world, 6 felt they could usually sense this risk with the remaining marking 'sometimes' (n=3), 'rarely' (n=2) or 'never' (n=4/15). Many participants (P1-7, 10-15) were worried about using the Internet, particularly due to concerns of some unknown (**who**) "Big Brother" watching them. "*[Your] phone can hear you anytime you don't know, everything is connected... I find it very frightening, very worrying*", said P7. Six participants (P4-6, 13-15) worried about **what** happens to the information they put on the Internet, **who** gets the access, **what** do they do with it once they get access, and **how** long do they keep it for. P4 said, "*I must*

admit, we are very casual. While searching for some accommodation, while planning travel, within seconds we start getting ads." P5 expressed negative emotions of anxiety and embarrassment that he had felt due to lack of awareness of **how** his information got leaked and **when** it could come back to disturb him. "*I came back from holidaying in Russia and sent photos to email of someone whom we met there. Thereafter, I started getting ads/alerts for pornographic websites and it appeared they are from Russia. We went to China, came back and I started receiving emails from Hong Kong. Just wondered how! Worry if such things pop up when I am with children*", said P5. Some (P13, P15) even showed concerns and desired more information on **what** happens to their personal information in the cloud after they die: "*Does it become the property of the cloud? I feel annoyed with it. A friend of mine died, but even after she was shown on a social site as coming to the birthday party. Her son wanted to take that down but couldn't. That is not fair*" [P13].

In addition to the usual aspects of 'access', that is: who, what, why, when and how, our participants also lacked awareness of the available tools or how to operate them, thereby resulting in high vulnerability. Six participants (P1, 2, 10-13) did not even have anti-malware software installed on their devices or had expired versions. They did not know how to install this software and were also unsure as to why they should have it (P7, 8). Participants were also unaware that their credentials are stored in the devices and websites they use if they don't logout. Those who used technologies like contactless payment cards were not aware that these could be used accidentally (or intentionally) to pay for someone else's shopping (P2, 13, 15). They were also not aware of how to protect such cards using devices like shielding covers. Participants were also found to seriously lack technical know-how in using existing technologies for privacy management. During the second part of the focus groups, we asked every participant to go to the privacy settings of their device and browser and turn on 'do not track' and delete 'cache and history' items. The majority of our participants (except P3, 9, 14 15) were unable to complete this task and had no idea of where they could find these settings. They agreed that they didn't know how to reach the privacy settings of different applications and didn't realize what and how much information was being taken.

Many (P1-6, 10-15) desired informative sessions on privacy like ours as they found the focus group discussions to be very helpful, "*eye-opener*" and "*nerve wracking but very informative*" (P1, 2). Some participants (P4, 5, 13-15) also suggested to use personal letters, local notice boards or even local daily newspapers with non-technical granny language style explanations (a) to specifically raise their general levels of privacy awareness, (b) to inform them about available technological tools for privacy-protection, and (c) to inform them about how to use those tools.

5.6.2 Privacy Control

The heightened vulnerability led to limited mitigation approaches. Seven participants said that they were heavily *dependent on others* such as their family members (P4, 6, 15), friends (P11, 13), neighbors (P7, 8) or even supermarket staff (P7, 8) to help them use digital devices and manage online privacy: "*Whenever I think there is issue with privacy or things like that, I have got people to call who can advise me on what to do in different situations*" [P15]. While depending on others for personal privacy management tasks can give older adults an opportunity to have a social interaction, it forces them to trust others, possibly including strangers. This increases the possibilities of undesired observations. Moreover, this support structure is not available to everybody. Furthermore, it is also not a desirable state when older adults are concerned about their independence and autonomy [77].

A lack of control over access to personal information by unknown entities (leading to identity theft, disclosure of financial details, etc.) has been widely reported in the literature as a barrier for older adults to adopt and use the Internet [22,27,58]. To protect online privacy and subsequent implications in the physical world, many often kept their Internet usage to a minimum. Seven participants (P1, 2, 7, 8, 11, 12, 14) reported minimal sharing of personal information over social networking sites especially when travelling as they were afraid of having that information passed to burglars and then getting burgled: "*It is not good to share your holiday pictures while you are still on holiday. This might give burglars a chance"* [P1]. This however restricted their chance to share even when they wanted to, thereby creating an imbalance in the bi-directional privacy continuum (where too much privacy or lack of social interaction can lead to social isolation [2]). P12, P14 and P15 also described restricting the information they used in online forms, sometimes giving fake information. For example, P14 once gave her cat's name instead of her own.

A few participants were able to use very *basic technological aids* to help them protect their privacy. These were limited to having, antivirus software installed on their desktop computers (P3, P4-9, P13-15), pre-setting

privacy settings (P3, 9, 14, 15), CCTV or having an alarm system installed at home (P1, 2, 4), using a RFID-shielding card defender (P2, 4), using a credit card instead of a debit card (P1-3, 13-15), and online privacy monitoring services (P3, 14).

Overall, participants either couldn't protect their privacy (as evident through many personal stories) or tried to naturally organize their limited control actions into allowing, blocking, confronting or recording the access and followed both reactive and proactive approaches.

a. Allow the access

Participants who used the Internet tried to trust certain services (**who**) and chose to compromise for convenience over privacy. Some allowed access **when** they saw greater benefits without any substantial negative implications. For example, P10 had allowed remote access (**how**) to her personal device (**what**) a couple of times to get her desktop repaired (**why**). P11 had a small home monitoring system which she was happy with to collect her information, "*This is for my benefit and happy for it to monitor me... it is also about social interaction. Nobody else cares so whatever this is, is fantastic*". This is interesting given that P11 described herself as having privacy concerns 'multiple times a day'. A few (P2, P4, 11) who mentioned social isolation as one of their challenges, also mentioned the need to open up and willingness to be accessed for greater interaction with others.

b. Block and Avoid the access

To protect from shoulder surfing of their ATM pin by a person or CCTV cameras (**who**), very few (P1, 10) reported being in the habit of covering their hand while entering pin at the ATM. Some reported to avoid using ATM when there were people around the ATM, or to wait until they were alone (P5, 7, 12). All avoided using such public cyber-physical devices in dark areas.

When the perceived costs were higher, participants simply attempted to block and avoid incoming observations or disturbances. P7 and P12 expressed concerns over **what** information might leak due to Internet banking and thus to control, decided not to use it. P1 and P5 did not use Wi-Fi outside their homes, as they knew the networks were not secure and they can't do anything about it: "*I am worried about that very much… afraid to use debit or credit card outside*" [P1]. Spam phone calls and posts regularly disturbed the participants (P4, 6, 10, 12-15). "*Spam calls just annoy me because you get up and go and get the phone. Stops you from doing from something else. Such spam calls come every day to me in the evening*" [P4]. Spam calls irritated P8 very much: "*They are generally selling some service. I will get it when I need. They keep calling anytime… This is a major violation of privacy*". Many depended on their instincts to sense and block access to their information by spam callers. P4 described: "*Once someone called me and said my computer is broken. They asked me to go on TeamViewer, which would give them control over my desktop and they can access anything. When I asked how much it is going to cost, the answer was enough to make me realize that something is fishy, and I cut it off*". P15 had a similar call from someone pretending to be from a named telecom company and offering help to fix her Internet through remote access. She had no issues with her Internet and was quick to sense something was wrong, leading her to hang up. However, the person called back again and questioned her aggressively as to why she put the phone down. To control such nuisance calls, two participants (P4, 11) tried to remember numbers ending with certain digits and not answer calls from those numbers. This did not always work as not only did they forget the numbers quite often but the spam calling numbers also kept changing.

c. Record the access

Several participants (P1, 2, 4, 13-15) discussed their concerns over 'cold callers' (**who**), people who come to their doorsteps trying to sell something (**why**). To regulate such physical access to their houses (**what**), some participants (P1, 2, 4) reported using CCTV surveillance systems for constant recording and using it later to report to their support network or authorities if needed. Group 2 expressed their comfort in having CCTV for surveillance in certain public locations as these could record and provide proof of committed crimes.

d. Confront (fight back)

CCTV cameras also acted as physical entities or extensions of users themselves that confronted the attacker, creating a socio-cultural situation of *you-know-that-I-know-that-you-know*. Such phenomena has been found to be effective in holding people accountable for their actions thereby improving their social behaviours [23]. A few participants (P5, 6, 15) mentioned not allowing waiters (**who**) to take their card (**what**) **when** paying

the bill in a restaurant and instead accompanying them. Four participants (P4, 6, 8, 14) reported confronting adversaries verbally on various occasions when they felt intruded and disturbed through spam calls. P6 once complained harshly to a spam caller (**who**) and hung up on him. "*To me it was an intrusion to my privacy in home. It should be me who must be given the opportunity to decide who can call to my home phone.*" [P6]. P4 reported her spam caller to the authorities. P14 reported sending junk mails back to people or organizations from where it had come.

The results under privacy awareness and control confirm the need to have interactive systems that can raise users' awareness about: different aspects of access (who, what, when, why and how), available controls and how to execute them. It also confirms the desire among the users to control the aspects of access through different regulatory mechanisms that come naturally to them. The modules of awareness and control in our Privacy Care framework cover these aspects and mechanisms.

5.6.3 Interaction Challenges

Many participants expressed difficulties in understanding technical terms and how to use state-of-the art technology, often referring to their age: "*No one has taught me how to use it properly. We didn't grow up with them... its' annoying when I can't use it [smartphone]*" [P4]. Some (P4, 5, 15) even felt embarrassed in front of children/grandchildren at times due to their inability to handle these devices. P11 raised concerns about the complexity of the instruction booklets that come with the devices. "*We don't understand instructions. You grew up with them, we didn't*" said P11 and suggested that the instructions should be in "*granny language*". P10 and 12 agreed with this. The complexity of multiple windows and menu based structures of GUI based systems, where a user needs to learn and remember sequences of multi-step tasks, manipulate images or patterns mentally, and process loads of information has been found to be cognitively demanding by researchers in the past [68,78]. This often leads to increased difficulties and reduced desirability to use such technologies [17], particularly amongst older adults.

Several participants (P2, 4-7, 10-13) noted critical interactional and usability challenges, that they particularly faced when trying to manage their privacy with existing technologies. Many participants (P2, P5, P7, P8, P12-14) had to increase their suspicion levels and felt paranoid particularly in dealing with their personal and financial details on the Internet. *"...always thinking or worried about what are they trying to find about me..."*, said P14. Interactions for privacy management were felt "hidden inside" the smartphone and difficult to access. Even password management was considered to be highly cumbersome and challenging. Seven participants (P1-4, 6, 10, 12) were not aware of best practice and consequently did not follow them. "*Where do you go to change the password?*" asked P6. Participants also reported difficulties in having different passwords for everything, changing them every now and then and keeping track of all of them: "*It is really too much sometimes... It is a real challenge...*" [P3]. Six participants (P1, 2, 4, 6, 10, 12) kept the same password for everything and never changed it. P4 considered it too much hassle to change passwords and didn't believe that it would make much of a difference: "*We have just learned to use the damn thing (smartphone) and there are so many traps... passwords are complex to form and remember... you press wrong buttons or don't remember... if you enter wrong password then it locks the system... have to then wait for mail to come and can't get on... too much frustrating...*"

a. Intuitiveness

Participants faced difficulties in learning, memorizing and navigating through technical jargon filled representations and operate them to manage their disclosure. Six participants (P1, 2, 4, 8, 11, 13) mentioned that even though their friends or relatives told them occasionally how to manage settings of their devices, they found it difficult to remember the sequence or found it complex due to multiple things "*hidden inside this [smartphone]*" [P4]. P1 quoted, "*It is frightening to access the privacy settings... where do I go*". Once logged out accidentally of applications like email or VoIP, some found it hard to log back in (P1, 2, 10, 13).

Intuitiveness was naturally found to be in more familiar acts. Some participants (P7, P12,13,15) found using cheques much intuitive than Internet banking but got ridiculed due to changed social expectations. For example, P13 mentioned people looking at her as if she "*were a dinosaur*" when they realized that she doesn't use Internet banking but cheques. Similarly, P15 argued that signing on physical paper is more direct and easier than using new techniques like contactless cards. More tangible style interfaces have also been suggested previously for reducing the interaction complexity, lowering the threshold for use and promise higher technology acceptance by older adults [39,44,79].

b. Granularity

Many demanded highly coarse and direct mechanisms of awareness and control to avoid being overwhelmed by the information on each and every access. For instance, P1 did not want to know about every access every time, but desired to just go to a maximum of two places to check their privacy settings for everything. Similarly, P2 wanted to have just an on/off button to control her information flow on systems such as for health monitoring and not have to micromanage. A few participants (P1, 2, 9) suggested quick access to coarse interactions by having a vibration system to warn themselves in real-time of a possible physical intrusion by disturbers such as 'cold callers', followed by a loud sound feedback to scare the adversary away. Similarly, quick, coarse and easy to access interactions such as on/off buttons were also understood to be highly desirable and useful in situations, where users have dependency on others for assistance with privacy management in their personal device. For instance, when an older adult approaches someone at the supermarket for help with her digital device, she could be given an opportunity to hide everything that is not required to be seen for receiving the help needed, in a one or maximum two step interaction. A couple of participants (P3, P5) also reported using more fine-grained controls by reading terms and conditions of digital applications and services and then choosing what to do.

c. Customizability to Context

No interactional problems in relation to the context were explicitly stated, except age related decline in physical (e.g. eyesight, dexterity, delayed reaction times) and cognitive abilities (e.g. memorizing mitigation approaches ad-hoc) which made it harder for some older adults to manage their privacy, especially in ad-hoc real-time scenarios. Previous research suggests older adults can have difficulties when interacting with capacitive [24] and resistive touch screens [64]. A lack of haptic feedback in such interfaces can create perceptual difficulties for older adults, especially those with dementia [87].

Nonetheless, all the user stories give us insights into different daily life ubicomp contexts of the participants. Inspirations can be drawn from such stories to design for systems that are appropriately customizable to fit into their context and create socially meaningful experience for the user. For instance, many participants in this user group uniquely experienced "social decline" – including the loss of a spouse or close family/friends, the loss of income and loneliness. To deal with occasional loneliness, many expressed the desire to open up and have more social interactions. This exposed them to having interactions with con callers (who often target their attack to this group) as well, as expressed by P2: "*When a person is lonely and gets a con call, there is a high possibility that they might be willing to talk to a stranger, as they haven't spoken to anyone for that whole day. This makes them very vulnerable... it could be dangerous... they could share a lot of personal details...*". The end-user privacy management system in such scenarios would have to find appropriate (intuitive and granular) ways to alert users of possible implications (e.g. information leakage, physical access to their house or even burglary), being mindful at the same time of the socialization needs of the user and encouraging (not discouraging) them from making new social connections. The system would need to sit in the background and act as a *guardian angel* who is there to guide and protect if things go wrong but doesn't disrupt the social interactions and make the user feel lonelier.

5.7 Summary

As the global population is ageing (around 960 million people aged 60 and above in 2017, expected to rise to 2 billion by 2050 [80]), researchers have started focusing on the needs of this specific user group. While many IoT technologies are being designed to help older adults successfully and independently age in place, the ubiquity of such technologies also exposes them to serious privacy threats. To reduce their vulnerability and increase technology acceptance, there is a strong need to design Privacy Care systems for this group.

To understand their real pain-points, we investigated the real-life privacy concerns faced by our focus group participants, as well as the mitigation approaches and constraints they faced in managing privacy. The participants were found to be highly prone to undesired observations and disturbances in a variety of everyday UbiComp contexts, due to lack of appropriate awareness and control. The results discussed under privacy awareness and control confirm the need to have interactive systems that can raise users' awareness about: different aspects of access (who, what, when, why and how), available controls and how to execute them. It also confirms the desire among the participants to control the aspects of access through different regulatory mechanisms that come naturally to them. The modules of awareness and control in our Privacy Care framework, cover these aspects and mechanisms. The sessions also unraveled several interactional challenges

that the participants faced with existing UIs for privacy management. They expressed their interaction experience to be complex, time-consuming and not available when needed and desired more (a) direct, intuitive, (b) granular and (c) customizable interactions. These needs are covered and addressed by direct, ready-to-hand and contextual elements of our framework.

The conformity of the focus groups results to the elements of our framework demonstrates its' usefulness in understanding the privacy routines and perceptions of this specific user group. It further guides the designers of privacy management tools on specific elements to consider when designing to improve the overall interactional and usability experience of this user group in UbiComp environments. Once the designers understand the unique challenges of a specific population, they can improve technology for both the specific and the broader population [19]. Hence, we hope that our framework can be used to design for effective and seamless privacy management in everyday contexts for users in other age groups as well.

6 Conclusion

In this paper, we highlight the interactional challenges that users face when trying to manage their privacy dynamically in everyday UbiComp contexts. Focusing on the user experience, we propose the use of more tangible and embodied style interactions and present the Privacy Care interaction framework. The framework is rooted in the literature of privacy and tangible computing and promises the provision of an *embodied* experience that is *Direct*, *Ready-to-Hand* and *Contextual* for effectively raising awareness and empowering users with seamless control. Our framework thus contributes to the bigger research agenda of usable privacy and security. Interaction designers can utilize the framework to come up with appropriate design concepts. The resulting designs could then guide software engineers on the functionalities to program into privacy-aware systems and hardware engineers on the form-factors and modalities that are desirable.

Through five semi-structured focus groups, we investigated the privacy challenges faced by a sample set of 15 older adults (aged 60+) across their cyber-physical-social spaces. The results conform to our framework, thereby demonstrating its' usefulness in real-life UbiComp contexts. Our next study will explore how the framework supports designers to empathize with, explore and generate designs for privacy management tools that are effective and can seamlessly integrate in the daily routines of its' users. We would encourage other researchers to use our framework to think about their approach to develop privacy management tools, and to provoke reflection about how they conceptualize individuals' experiences of privacy in UbiComp contexts.

ACKNOWLEDGMENTS

This work was completed with support from EPSRC grants EP/P01013X/1 and EP/R013144/1 as well as SFI grant 13/RC/2094 and 16/SP/3804.

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. *Environ. Behav.* 8, 1 (1976), 7–29.

[3] S Saskia Bakker. 2013. Design for peripheral interaction. (2013). DOI:https://doi.org/10.6100/IR754544

[4] Saskia Bakker, Elise van den Hoven, and Berry Eggen. 2015. Peripheral interaction: characteristics and considerations. *Pers. Ubiquitous Comput.* 19, 1 (January 2015), 239–254. DOI:https://doi.org/10.1007/s00779-014-0775-2

[5] 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. Retrieved April 20, 2017 from http://dl.acm.org/citation.cfm?id=2501616

[6] Julia Barrett and Stuart Kirk. 2000. Running focus groups with elderly and disabled elderly participants. *Appl. Ergon.* 31, 6 (2000), 621–629.

[7] ayah bdeir. 2006. random search. *random search*. Retrieved from http://ayahbdeir.com/work/random-search/

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

[9] 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. DOI:https://doi.org/10.1007/978-94-011-2094-4_6

[10] Michael Boyle and Saul Greenberg. 2005. The language of privacy: Learning from video media space analysis and design. *ACM Trans. Comput.-Hum. Interact.* 12, 2 (June 2005), 328–370. DOI:https://doi.org/10.1145/1067860.1067868

[11] Christian Bunnig and Clemens H. Cap. 2009. Ad Hoc Privacy Management in Ubiquitous Computing Environments. In *2009 Second International Conference on Advances in Human-Oriented and Personalized Mechanisms, Technologies, and Services*, IEEE, Porto, Portugal, 85–90. DOI:https://doi.org/10.1109/CENTRIC.2009.20

[12] 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. *J. Soc. Pers. Relatsh.* 6, 2 (May 1989), 131–158. DOI:https://doi.org/10.1177/026540758900600201

[13] Sangmi Chai, HR Rao, S Bagchi-Sen, and S Upadhyaya. 2008. 'WIRED'SENIOR CITIZENS AND ONLINE INFORMATION PRIVACY. *Living Work. Learn. Beyond* (2008), 101.

[14] R Chakraborty, HR Rao, and SJ Uphadhyahy. 2010. BANDES: an adaptive decision support system for protecting online privacy for senior citizen centers. In *fourth Pre-ICIS workshop on information security & privacy (WISP)–the official annual workshop of association of information systems SIG/SEC.* Retrieved from http://www. security-conference. org/sigsec/WISP2009papers/4. pdf. Accessed

[15] Jessica Colnago and Hélio Guardia. 2016. How to inform privacy agents on preferred level of user control? ACM Press, 1542–1547. DOI:https://doi.org/10.1145/2968219.2968546

[16] 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.

[17] Sara J. Czaja and Chin Chin Lee. 2007. The impact of aging on access to technology. *Univers. Access Inf. Soc.* 5, 4 (March 2007), 341–349. DOI:https://doi.org/10.1007/s10209-006-0060-x

[18] Paul Dourish. 2001. *Where the Action Is: The Foundations of Embodied Interaction*. The MIT Press. DOI:https://doi.org/10.7551/mitpress/7221.001.0001

[19] Paul Dunphy, John Vines, Lizzie Coles-Kemp, Rachel Clarke, Vasilis Vlachokyriakos, Peter Wright, John McCarthy, and Patrick Olivier. 2014. Understanding the Experience-Centeredness of Privacy and Security Technologies. In *Proceedings of the 2014 New Security Paradigms Workshop*, ACM Press, 83–94. DOI:https://doi.org/10.1145/2683467.2683475

[20] Darren Edge and Alan F. Blackwell. 2009. Peripheral tangible interaction by analytic design. ACM Press, 69. DOI:https://doi.org/10.1145/1517664.1517687

[21] Berry Eggen, Koert van Mensvoort, David Menting, Emar Vegt, Wouter Widdershoven, and Rob Zimmermann. Soundscapes at Workspace Zero – Design Explorations into the Use of Sound in a Shared Environment. 8.

[22] Isioma Elueze and Anabel Quan-Haase. 2018. Privacy attitudes and concerns in the digital lives of older adults: Westin's privacy attitude typology revisited. *ArXiv Prepr. ArXiv180105047* (2018).

[23] Thomas Erickson and Wendy A. Kellogg. 2000. Social translucence: an approach to designing systems that support social processes. *ACM Trans. Comput.-Hum. Interact. TOCHI* 7, 1 (March 2000), 59–83. DOI:https://doi.org/10.1145/344949.345004

[24] Stu Favilla and Sonja Pedell. 2013. Touch screen ensemble music: collaborative interaction for older people with dementia. ACM Press, 481–484. DOI:https://doi.org/10.1145/2541016.2541088

[25] 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. Retrieved December 7, 2016 from http://dl.acm.org/citation.cfm?id=2335360

[26] Alois Ferscha, Manfred Hechinger, Rene Mayrhofer, Marcos dos Santos Rocha, Marquart Franz, and Roy Oberhauser. 2004. Digital aura. (2004). Retrieved April 25, 2017 from http://pervasive2004.soft.uni-linz.ac.at/Research/Publications/_Documents/DigitalAura-ferscha2004.pdf

[27] Susan L. Gatto and Sunghee H. Tak. 2008. Computer, Internet, and E-mail Use Among Older Adults: Benefits and Barriers. *Educ. Gerontol.* 34, 9 (August 2008), 800–811. DOI:https://doi.org/10.1080/03601270802243697
[28] James J Gibson. 2014. *The ecological approach to visual perception: classic edition*. Psychology Press.
[29] Saul Greenberg and Hideaki Kuzuoka. 1999. Using digital but physical surrogates to mediate awareness, communication and privacy in media spaces. *Pers. Technol.* 3, 4 (1999), 182–198.
[30] Doris Hausen and Andreas Butz. Extending Interaction to the Periphery. 5.
[31] Martin Heidegger. 1996. *Being and time: A translation of Sein und Zeit*. SUNY press.
[32] Eva Hornecker and Jacob Buur. 2006. Getting a grip on tangible interaction: a framework on physical space and social interaction. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, ACM, 437–446.
[33] Scott E. Hudson, Chris Harrison, Beverly L. Harrison, and Anthony LaMarca. 2010. Whack gestures: inexact and inattentive interaction with mobile devices. In *Proceedings of the fourth international conference on Tangible, embedded, and embodied interaction - TEI '10*, ACM Press, Cambridge, Massachusetts, USA, 109. DOI:https://doi.org/10.1145/1709886.1709906
[34] Jörn Hurtienne and Johann Habakuk Israel. 2007. Image schemas and their metaphorical extensions: intuitive patterns for tangible interaction. ACM, 127–134.
[35] 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. *Interact. Comput.* 22, 6 (November 2010), 475–484. DOI:https://doi.org/10.1016/j.intcom.2010.08.009
[36] Hiroshi Ishii. 2008. Tangible bits: beyond pixels. In *Proceedings of the 2nd international conference on Tangible and embedded interaction*, ACM, xv–xxv. Retrieved October 12, 2017 from http://dl.acm.org/citation.cfm?id=1347392
[37] Hiroshi Ishii and Brygg Ullmer. 1997. Tangible bits: towards seamless interfaces between people, bits and atoms. In *Proceedings of the ACM SIGCHI Conference on Human factors in computing systems*, ACM, 234–241.
[38] 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. *Int. J. Arts Technol.* 2, 4 (2009), 348. DOI:https://doi.org/10.1504/IJART.2009.029240
[39] Thomas René Iversen and Suhas Govind Joshi. 2015. Exploring Spatial Interaction in Assistive Technology Through Prototyping. *Procedia Manuf.* 3, (2015), 158–165. DOI:https://doi.org/10.1016/j.promfg.2015.07.121
[40] Lukasz Jedrzejczyk. 2012. Supporting Location Privacy Management through Feedback and Control. PhD Thesis. The Open University.
[41] 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. Retrieved from http://dl.acm.org/citation.cfm?id=1851690
[42] 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. ACM Press, 411. DOI:https://doi.org/10.1145/1851600.1851690
[43] Mark Johnson. 2013. *The body in the mind: The bodily basis of meaning, imagination, and reason*. University of Chicago Press.
[44] Suhas Govind Joshi and Heidi Bråthen. 2016. Lowering the threshold: reconnecting elderly users with assistive technology through tangible interfaces. Springer, 52–63.
[45] Daniel Kahneman. 1973. *Attention and effort*. Prentice-Hall, Englewood Cliffs, N.J.
[46] 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. Retrieved December 16, 2016 from http://link.springer.com/10.1007/978-3-540-72037-9_10
[47] Predrag Klasnja, Sunny Consolvo, Jaeyeon Jung, Benjamin M Greenstein, Louis LeGrand, Pauline Powledge, and David Wetherall. "When I am on Wi-Fi, I am Fearless:" Privacy Concerns & Practices in Everyday Wi-Fi Use. 10.

[48] Bastian Könings. 2015. User-centered awareness and control of privacy in Ubiquitous Computing. PhD diss. PhD diss., Universität Ulm.
[49] Richard A Krueger and Mary Anne Casey. 2014. *Focus groups: A practical guide for applied research*. Sage publications.
[50] Ponnurangam Kumaraguru and Lorrie Faith Cranor. 2005. Privacy indexes: a survey of Westin's studies. (2005). Retrieved January 25, 2017 from http://repository.cmu.edu/isr/856/
[51] Marc Langheinrich. 2002. Privacy invasions in ubiquitous computing. In *Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing. UbiComp*, Citeseer. Retrieved October 17, 2016 from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.6.6743&rep=rep1&type=pdf
[52] Scott Lederer. 2003. Designing Disclosure: Interactive Personal privacy at the Dawn of ubiquitous computing. *Unpubl. Master Sci. Univ. Calif. Berkeley Berkeley CA Httpwww Cs Berkeley Eduprojectsiopublicationsprivacy-Lederer-Msreport-101-No-Append. Pdf* (2003).
[53] Scott Lederer, Anind K Dey, and Jennifer Mankoff. A Conceptual Model and a Metaphor of Everyday Privacy in Ubiquitous Computing Environments. 9.
[54] Jaakko T. Lehikoinen, Juha Lehikoinen, and Pertti Huuskonen. 2008. Understanding privacy regulation in ubicomp interactions. *Pers. Ubiquitous Comput.* 12, 8 (November 2008), 543–553. DOI:https://doi.org/10.1007/s00779-007-0163-2
[55] Saija Lemmelä, Akos Vetek, Kaj Mäkelä, and Dari Trendafilov. 2008. Designing and evaluating multimodal interaction for mobile contexts. In *Proceedings of the 10th international conference on Multimodal interfaces - IMCI '08*, ACM Press, Chania, Crete, Greece, 265. DOI:https://doi.org/10.1145/1452392.1452447
[56] 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.
[57] Christian Loclair, Sean Gustafson, and Patrick Baudisch. PinchWatch: A Wearable Device for One-Handed Microinteractions. 4.
[58] Wiebke Maaß. 2011. The elderly and the Internet: How senior citizens deal with online privacy. In *Privacy online*. Springer, 235–249.
[59] 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. DOI:https://doi.org/10.1145/332040.332438
[60] John McCarthy and Peter Wright. 2010. The Critical Potential of Experience in Experience-Centered Design. In *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*, ACM Press, 6.
[61] Vikram Mehta. 2020. Privacy Care - study repository. Retrieved from , https://github.com/PrivacyCare/Study
[62] 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. DOI:https://doi.org/10.1145/2851581.2892475
[63] 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*, SAGE Publications Sage CA: Los Angeles, CA, 266–270.
[64] Lilian Motti, Vigouroux Nadine, and Philippe Gorce. Interaction techniques for older adults using touchscreen devices: a literature review from 2000 to 2013. 3, 2 , 29.
[65] David H Nguyen and Elizabeth D Mynatt. 2002. *Privacy mirrors: understanding and shaping socio-technical ubiquitous computing systems*. Georgia Institute of Technology.
[66] Fernando Olivera, Manuel García-Herranz, Pablo A. Haya, and Pablo Llinás. 2011. Do Not Disturb: Physical Interfaces for Parallel Peripheral Interactions. In *Human-Computer Interaction – INTERACT 2011*, Springer Berlin Heidelberg, Berlin, Heidelberg, 479–486.
[67] Leysia Palen and Paul Dourish. Unpacking "Privacy" for a Networked World. 8.
[68] Robert Pastel, Charles Wallace, and Jesse Heines. 2007. RFID Cards: A New Deal for Elderly Accessibility. In *Universal Acess in Human Computer Interaction. Coping with Diversity*, Constantine Stephanidis (ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 990–999. DOI:https://doi.org/10.1007/978-3-540-73279-2_111

[69] James Ponsoldt. 2017. *The Circle*. Retrieved from http://thecircle.movie
[70] Florian Schaub and Pascal Knierim. Drone-based Privacy Interfaces: Opportunities and Challenges. 4.
[71] Roman Schlegel, Apu Kapadia, and Adam J. Lee. 2011. Eyeing your exposure: quantifying and controlling information sharing for improved privacy. ACM Press, 1. DOI:https://doi.org/10.1145/2078827.2078846
[72] Albrecht Schmidt, Michael Beigl, and Hans-W. Gellersen. 1999. There is more to context than location. *Comput. Graph.* 23, 6 (1999), 893–901.
[73] Elisabeth SchröDer-Butterfill and Ruly Marianti. 2006. A framework for understanding old-age vulnerabilities. *Ageing Soc.* 26, 01 (January 2006), 9–35. DOI:https://doi.org/10.1017/S0144686X05004423
[74] Orit Shaer. 2009. Tangible User Interfaces: Past, Present, and Future Directions. *Found. Trends® Human–Computer Interact.* 3, 1–2 (2009), 1–137. DOI:https://doi.org/10.1561/1100000026
[75] Ben Shneiderman. 1993. 1.1 direct manipulation: a step beyond programming languages. *Sparks Innov. Hum.-Comput. Interact.* 17, (1993), 1993.
[76] Carolyn M Shrewsbury. 2002. Information technology issues in an era of greater state responsibilities: policy concerns for seniors. *J. Aging Soc. Policy* 14, 3–4 (2002), 195–209.
[77] Andrew Sixsmith. 1986. Independence and home in later life. *Depend. Interdepend. Old Age Theor. Perspect. Policy Altern.* (1986), 338–347.
[78] Wolfgang Spreicer. 2011. Tangible interfaces as a chance for higher technology acceptance by the elderly. ACM, 311–316.
[79] Wolfgang Spreicer. 2011. Tangible interfaces as a chance for higher technology acceptance by the elderly. In *Proceedings of the 12th International Conference on Computer Systems and Technologies*, ACM, 311–316.
[80] United Nations, Department of Economics and Social Affairs, and Population Division. 2017. *World population ageing, 2017 highlights*.
[81] Emanuel Vonach, Georg Gerstweiler, and Hannes Kaufmann. 2014. ACTO: A Modular Actuated Tangible User Interface Object. In *Proceedings of the Ninth ACM International Conference on Interactive Tabletops and Surfaces - ITS '14*, ACM Press, Dresden, Germany, 259–268. DOI:https://doi.org/10.1145/2669485.2669522
[82] Wei Wang, Lin Yang, and Qian Zhang. 2016. Touch-and-guard: secure pairing through hand resonance. ACM Press, 670–681. DOI:https://doi.org/10.1145/2971648.2971688
[83] Mark Weiser and John Seely Brown. Designing Calm Technology. 5.
[84] Stephan AG Wensveen, Johan Partomo Djajadiningrat, and C. J. Overbeeke. 2004. Interaction frogger: a design framework to couple action and function through feedback and feedforward. In *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques*, ACM, 177–184.
[85] Christopher D. Wickens. 2008. Multiple Resources and Mental Workload. *Hum. Factors J. Hum. Factors Ergon. Soc.* 50, 3 (June 2008), 449–455. DOI:https://doi.org/10.1518/001872008X288394
[86] Peter Wright and John McCarthy. 2010. Experience-centered design: designers, users, and communities in dialogue. *Synth. Lect. Hum.-Centered Inform.* 3, 1 (2010), 1–123.
[87] Christina Yamagata, Jean F. Coppola, Marc Kowtko, and Shannon Joyce. 2013. Mobile app development and usability research to help dementia and Alzheimer patients. IEEE, 1–6. DOI:https://doi.org/10.1109/LISAT.2013.6578252
[88] John Zimmerman, Jodi Forlizzi, and Shelley Evenson. 2007. Research through design as a method for interaction design research in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '07*, ACM Press, San Jose, California, USA, 493–502. DOI:https://doi.org/10.1145/1240624.1240704
[89] Tomasz Zukowski and Irwin Brown. 2007. Examining the influence of demographic factors on internet users' information privacy concerns. In *Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries - SAICSIT '07*, ACM Press, Port Elizabeth, South Africa, 197–204. DOI:https://doi.org/10.1145/1292491.1292514