Tangible Interactions for Privacy Management

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

ABSTRACT
Due to the ubiquity of IoT devices, privacy violations can now occur across our cyber-physical-social lives. An individual is often not aware of the possible privacy implications of their actions and commonly lacks the ability to dynamically control the undesired access to themselves or their information. Present approaches to privacy management lack an immediacy of feedback and action, tend to be complex and non-engaging, are intrusive and socially inappropriate, and are inconsistent with users' natural interactions with the physical and social environment. This results in ineffective end-user privacy management. To address these challenges, I focus on designing tangible systems, which promise to provide high levels of stimulation, rich feedback, direct, and engaging interaction experiences. This is achieved through intuitive awareness mechanisms and control interactions, conceptualizing interaction metaphors, implementing tangible interfaces for privacy management and demonstrating their utility within various real life scenarios.

Author Keywords
Tangibles for privacy management; End-user privacy; Cyber-physical-social environments; Interaction design.

CONTEXT AND MOTIVATION FOR DISSERTATION
The ever-increasing proliferation of ubicomp systems in our everyday spaces has nurtured the growth of cyber-physical-social environments (CPSE). The private territory of an individual now expands beyond their physical boundaries to include virtual (cyber) territory [7]. Personal information can be sensed (or observed) from users' physical actions by observers (human and technological), and uploaded invisibly to the Internet without warning. The constant interaction with, and interruptions (or disturbances) from disturbers (human and technological) around a user can have a detrimental effect on their social relationships and mental wellbeing. Such observations and disturbances can be termed as privacy threats, which originate from the cyber, physical and social worlds that individuals inhabit. Many people are unable to perceive or control who is observing or disturbing them in their extended private territory, leading to a lack of awareness of possible privacy implications, resulting in inadequate protection practices.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.
TEI '19, March 17–20, 2019, Tempe, AZ, USA
© 2019 Copyright is held by the owner/author(s). Publication rights licensed to ACM.
ACM 978-1-4503-6196-5/19/03…$15.00
https://doi.org/10.1145/3294109.3302934

RESEARCH OBJECTIVES AND CHALLENGES
My research objective is to build solutions to enable end-users to effectively (in a proactive and reactive manner) manage privacy in CPSE. I identify the following challenges: **RC1:** To engage inexperienced users in privacy management. **RC2:** To actively (without overloading) raise awareness of potential violations without disrupting user's social and functional lives in runtime. **RC3:** To enable direct and intuitive controls without requiring them to go through high and technical learning curves.

BACKGROUND/LITERATURE REVIEW
Privacy is about managing the disclosure of ones' physical space and personal information to others. In the context of CPSE, it is an individual's right to be aware of potential observations and disturbances, and their right to control undesired ones [7]. Due to bi-directional nature of privacy [1], an individual may sometimes also experience too much privacy (social isolation).

Existing interfaces that support privacy awareness and control can be categorized into three non-exclusive sets: (1) UIs for online privacy [3], (2) UIs for mobile privacy [2], and (3) UIs for UbiComp privacy [7]. Through a wide survey of the end-user privacy management literature, I have determined that for a contextual task of privacy management, present approaches can lack immediacy of feedback and action, tend to be complex and non-engaging, and are inconsistent to users' natural interactions with the physical and social environment. The intrusive nature of many existing privacy alert mechanisms, and the cumbersome and non-discreet nature of existing privacy controls results in ineffective solutions.

Literature shows that Tangible User Interfaces (TUIs) hold the potential to provide high levels of realism and stimulation, rich feedback and intuitiveness of interaction to users. In the context of privacy, this is also supported by my early research on on-body privacy warnings and controls [8]. Tangible forms of interaction cover a range of computational 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 " [5]. I propose

to design such tangible interactions to enable end-users manage their privacy in complex scenarios of CPSE.

PROBLEM STATEMENT/RESEARCH QUESTION

Main research question is: **How can tangible interactions engage and enable end-users to continuously, intuitively and efficiently manage their territorial privacy in cyber-physical-social environments?**

"Manage" here refers to enhancing awareness and enabling control. I split the usability aspects into four features: engaging, continuous, intuitive and efficient. **"Engage"** means being able to involve users in managing their privacy in a delightful and pleasing manner. **"Continuous"** means the proposed solution must be able to actively raise user's awareness and enable control at all times whenever the user desires or is urgently required to manage their privacy. It should not annoy users through constant notifications. Information should be presented at different levels from coarse-grained to fine-tuned depending on how much the user wants to know and control. **"Intuitive"** means the ease of use in different contexts. It aims to make the interactions natural and direct to the user, without high (or technical) learning curves and cognitive load. "**Efficient**" means increasing the speed of use and reducing the number of steps required to manage privacy in a given context.

These features should be implemented and evaluated in cohesion to assess overall effectiveness of the proposed solution. Social appropriateness of the interaction should be considered, ensuring that awareness is raised through discreet methods, and to provide non-intrusive controls. I further divide the main research question into 2 sub-questions: (a) how can we exploit culturally specific or biologically grounded metaphors in the design of tangible interactions that raise awareness and enable control of privacy in daily settings? (b) How can we use alternative tangible modalities to raise awareness and enable control of privacy in daily settings?

SAMPLE PROBLEM SCENARIOS

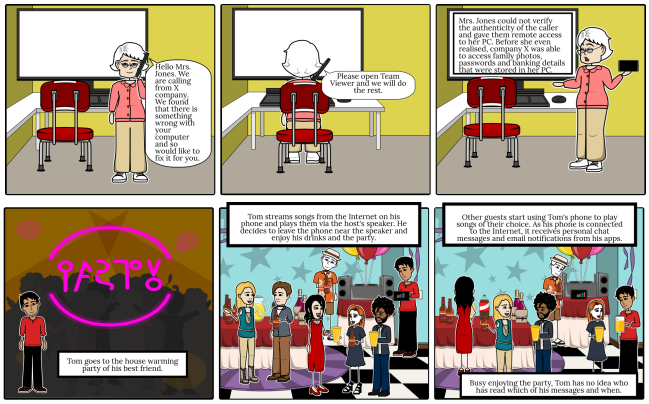

Figure 1: (a) fraud calls to gain access to remote desktop, (b) access to personal device by someone in a party

In figure 1, I illustrate two real-life scenarios where privacy management is practically challenging.

RESEARCH APPROACH AND METHODS

Privacy is highly personal and contextual in nature. To design effective methods and tools I keep end-users at the center of my research approach. My research includes three basic activities of interaction design: (1) Identifying needs and establishing requirements, (2) Designing and building prototypes, and (3) Evaluation. To **identify user needs**, I am utilizing exploratory methods and findings from literature. In the **design & build** step, I am conceptualizing and designing cultural or biologically grounded metaphors and models that underpin the established socio-centric privacy theories into tangible approaches for interaction. I also plan to instantiate conceptual designs by building low and medium fidelity prototypes using off the shelf microelectronics, digital fabrication, software and other prototyping tools. I plan to **evaluate** user engagement, continuous nature, intuitiveness, efficiency and appropriateness of our proposed solutions through empirical methods involving lab and field-testing.

I follow an iterative and incremental approach and hence execute these activities in 3 phases (see figure 2). Findings from each phase inform future phases. Across all of these phases, I use a combination of common data collection techniques including questionnaires, structured and semi-structured interviews (one-to-one, focus group), participatory design (co-design workshops) and direct observations. Qualitative (e.g. thematic analysis) and quantitative methods (statistical analysis) are used for data analysis and to explore and identify significant patterns.

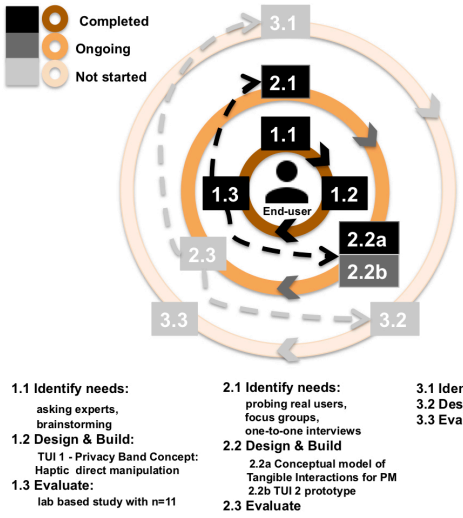

Figure 2: Iterative User-Centered Research Methodology

RESULTS TO DATE

Figure 2 also illustrates the status of my three-phased research. I have finished phase 1. Initial enquiry into the problem space was done through the exploratory literature review and brainstorming with experts. One key requirement was to provide users with subtle, real-time privacy warnings and non-obtrusive control capabilities. This is particularly important in social situations such as

when in meetings. To fulfill this, I designed and prototyped Privacy Band (see figure 3): 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 [8]. Initial work (lab user study with 11 participants) has shown that it can help raise the privacy awareness of its' user through discreet haptic vibrations (metaphorical 'privacy itch') at distinct locations and prompt them to react (or control) their privacy in an intuitive and immediate manner through direct manipulation (metaphorical 'privacy scratch').

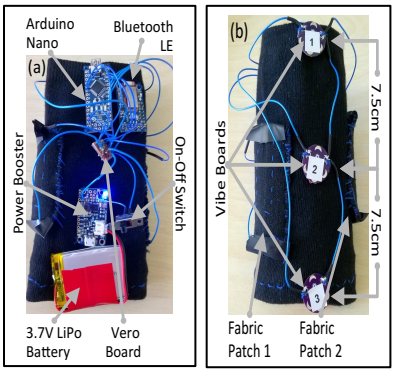

Figure 3: Privacy Band (a) "Front" view, (b) Back view

A sample scenario for Privacy Band: Adam has a wide network of friends and enables the Buddy Tracker app on his smartphone, which allows selected friends to locate him for serendipitous meetings. He wants to have some control over his privacy so he connects the Buddy Tracker app to the Privacy Band. While in a café with Bob he feels a slight itch on his forearm indicating that an observer has checked his location. He does not want his chat with Bob to be disturbed so he subtly scratches (haptic direct manipulation) the inner side of his forearm indicating that he wants to keep this information private and the Buddy Tracker app stops revealing his location. If instead he wanted to meet the observer at the café he could have scratched his outer forearm to indicate that he is happy for his location to be shared.

In the 2nd phase, I have explored the needs of end-users. Focusing on older adults (aged 60+), I have completed 5 focus groups (n=15) to explore the privacy concerns, mitigation approaches and challenges faced by them in CPSE. I found that older adults are highly prone to undesired observations and disturbances in their day-to-day living and these occur across cyber, physical and social spaces. They try to block and avoid, log, confront or even allow the access but face various challenges in doing so. There is a clear lack of technological solutions that are appropriate and sufficient for multiple contexts in CPSE. In addition, many are either not aware of the presence of existing tools for privacy management or are unable to interact with them. They desire regulated awareness and intuitive controls to manage their privacy. Based on the findings and literature, I have constructed a conceptual model (see figure 4) that can be used to design interfaces to help end-users manage privacy reactively and proactively.

The model consists of two integral components: Awareness and Control (see Table 1 and 2), which are inherent to any tangible interface [6], and are equally essential for the user's sense of personal privacy.

Awareness Component	
Mechanisms	1. Feed-back: report 2. Feed-forward: prompt
Medium (Modalities)	1. Tangible: Haptics (e.g. vibration, temperature) 2. Intangible: Peripheral vision, sound, smell
Features	1. Characteristics of access: a. People (who), b. Purpose (why), c. Method (what, when) 2. Time of awareness input: a. real-time, b. end-of-the-day 3. Position of awareness input: a. on-body, b. ambient

Table 1. Awareness Characteristics

Control Component	
Mechanisms (Actions)	1. Pro-act, 2. React
Medium (Modalities)	1. Direct manipulation, 2. Body postures, 3. Full body movements
Features	Forms of control: a. Allow, b. Block, c. Confront (fight back), d. Log

Table 2. Control Characteristics

Depending on the users' context (age, time, location, activity), capabilities (physical, cognitive, social and technical abilities), and privacy needs [4] (intimate, personal, social, public), when an external application senses potential privacy violation, it informs **(A.2, figure 4)** the digital element of the awareness (representation) component with characteristics of the violation or risk. Violations could span across cyber, physical and social spaces of the user. Some of the user's context, capabilities, privacy needs and preferences for notification and control, are manually fed into system at the time of setup **(A.1, figure 4)**. Those that change often can be sensed through TUI sensors or user's existing devices like smartphones.

Not all elements of potential access need to be informed to the user. Depending upon user's preference and context, the digital element also decides on the time and position to deliver the awareness notification (for e.g. discreet on-body notification when in meeting or ambient notification when sitting in a private cabin). This information can then,

tangibly or intangibly, be communicated (feed-forward) to the user to warn of a future threat or potential access as part of the physical element of the awareness system. The affordance of the tangible interface at that point prompts and guides **(A.3, figure 4)** the user to react (or control) **(A.4, figure 4)** their privacy in an intuitive and immediate manner through direct manipulation, body postures or full body movements. These interactions depend on users' preference, context and capabilities. I plan to investigate the suitable awareness and control modalities empirically.

The user could allow, block, confront or log the violations as per their context, capabilities and privacy needs. These user actions occur in the physical element of the control component. The system gives inherent feedback [9] to the user in scenarios that involve haptic direct manipulation. This restores (or helps collect evidence) **(A.5, figure 4)** of users' privacy and updates the digital and physical state of the tangible interface **(A.6, figure 4)**. In the end, the user receives functional feedback [9] **(A.7, figure 4)** of her actions (whether privacy has been restored as desired or not) through the awareness component.

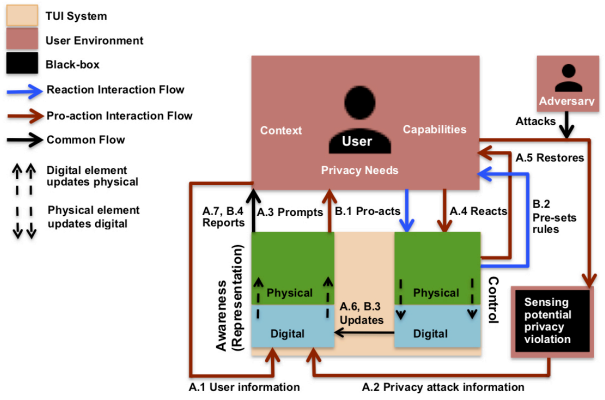

Figure 4. Conceptual Model for Designing Tools for End-User Privacy Management in CPSE.

Another possible flow is when user follows a proactive approach. In this case, the user may sense the need to control their privacy and pro-acts **(B.1, figure 4)** in a manner similar to the workflow described above. This may pre-set **(B.2, figure 4)** privacy rules/needs of the user and update **(B.3, figure 4)** the digital and physical state of the tangible interface. The system reports acknowledgment to the user through functional feedback **(B.4, figure 4)**.

DISSERTATION STATUS AND NEXT STEPS

I plan to continue with phase 2 activity of building an improved TUI prototype for privacy management. This will be followed by a simulated lab-based evaluation. 3rd phase will involve co-designing with end-users and developing the final prototype. Time permitting; I intend to conduct a field study involving carefully planned targeted privacy violations in the physical and digital environments of the participants. I plan to finish fieldwork by the beginning of 2020 and complete thesis writing by mid-2020.

CURRENT AND EXPECTED CONTRIBUTIONS

I have proposed the concept of tangible interactions for end-user privacy management. I have demonstrated the concept through implementing on-body interfaces for alerting users about personal privacy breaches, and providing them the ability to directly control the access to their information in a discreet and non-obtrusive manner. I plan to contribute an empirically grounded and validated model (substantiated with prototypes) to help designers build interfaces and interactions for effective end-user privacy management in CPSE. I also plan to use this model for generating relevant metaphors.

The concepts of Privacy as well as methods for violation and protection have evolved over time and need greater attention than ever before. With this research, I aim to empower end-users by providing them with intuitive, engaging, continuous and effective interaction methods and tools for managing privacy as and when desired.

ACKNOWLEDGEMENTS

My work is supported by ERC Advanced Grant 291652, EPSRC Grants EP/K033522/1 and EP/P01013X/1.

REFERENCES

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

[2] 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 *Proc of 9th SOUPS'13* , 12.

[3] Lorrie Faith Cranor, Praveen Guduru, and Manjula Arjula. 2006. User interfaces for privacy agents. *ACM TOCHI'06* 13, 2: 135–178.

[4] Edward T. Hall, Ray L. Birdwhistell, Bernhard Bock, Paul Bohannan, A. Richard Diebold Jr, Marshall Durbin, Munro S. Edmonson, J. L. Fischer, Dell Hymes, Solon T. Kimball, and others. 1968. Proxemics. *Current anthropology* 9, 2/3: 83–108.

[5] Eva Hornecker and Jacob Buur. 2006. Getting a grip on tangible interaction: a framework on physical space and social interaction. In *Proc of SIGCHI CHI'06*, 437–446.

[6] Hiroshi Ishii. 2008. Tangible bits: beyond pixels. In *Proc of the 2nd TEI*, xv–xxv.

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

[8] Vikram Mehta, Arosha K. Bandara, Blaine A. Price, and Bashar Nuseibeh. 2016. Privacy Itch and Scratch: On Body Privacy Warnings and Controls. In EA CHI'16, 2417–2424.

[9] 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 *Proc of 5th DIS* , 177–184.