ICED13
INTERNATIONAL CONFERENCE ON ENGINEERING DESIGN, ICED13
19-22 AUGUST 2013, SUNGKYUNKWAN UNIVERSITY, SEOUL, KOREA

DESIGN FOR PRIVACY – DESIGN TOOL TO MAP PERCEPTIONS, CONFLICTS AND STRATEGIES OF PRIVACY IN MOBILE TECHNOLOGY DEVELOPMENT

Diana SCHNEIDER (1), Tanja KORNBERGER (2)
1: Technical University of Munich, Germany; 2: Center for Digital Technology and Management, Germany

ABSTRACT
This paper investigates the area of tension of privacy versus technologically enabled ubiquity, in order to align both into improved product and service design solutions.
Through an iterative process combining theoretical, empirical and design research, using transdisciplinary methods from social sciences, design thinking and engineering, the authors propose a design tool to comprehend and visualize the implications of privacy in high-tech applications.
The empirical insights substantiating the theoretical classification system were gathered in two phases: (a) a survey-based quantitative study identifying mobile technologies as the main privacy concern and (b) an interview-based qualitative study with software developers further exploring privacy issues in mobile technologies.
The gathered theoretical and empirical insights were structured into a four-point "privacy in technology" reference model for mobile developers and design professionals to solve conflicts arising from the privacy/ mobile technology correlation. These four elements consolidate (1) privacy perceptions, (2) common mobile technology development processes, (3) privacy conflicts, (4) strategies to solve privacy concerns.

Keywords: privacy, ubiquity, mobile technologies, transdisciplinary methodology, design tool

Contact:
Diana Schneider
BriskRoad
Design Thinking
Sint-Pieters-Leeuw
1600
Belgium
diana.schneider@cdtm.de

1 INTRODUCTION - TRANSDISCIPLINARY APPROACH COMBINING THEORY AND EMPIRICISM

The alleged duality between privacy versus ubiquity/ publicity is a vastly discussed leitmotif in science, literature, media and everyday life and has been thus for two millennia (Sokol, 2001). The current scientific and mediatized examination of privacy highlights the protection of private places, people and data against the threats of the public eye, underestimating the necessity of a participative, interactive, healthy public sphere: a physical or virtual cornerstone of a functioning society (Harvard Symposium, 2011). Thus our motivation to examine *privacy* in a *public context*, exemplified by the field combining both: mobile technologies.

This paper aims at dissecting the interdependence between private and ubiquitous spheres in the context of mobile technologies. The latter have not only altered the understanding of privacy (Turkle, 2004), but also account for concerns with regards to user privacy (Barkhuus and Dey, 2003). By using a mixed-method approach combining social sciences, design thinking and engineering this research results in a tool that serves as a reference model for software developers and design professionals working on mobile application to help solve privacy-related issues along the development process.

To this end, this paper embarks on a multilevel strategy comprised of empirical and theoretical research. The first step involves mapping the theoretical understanding of privacy. This is realized through an extensive literature review, which explores the perceptions of privacy and the public sphere. Paired with a quantitative survey it results in a multi-layered model of privacy taking into consideration varying levels of interaction. Building upon this understanding of privacy, insights from the survey are further utilized to dissect the privacy layers and explore privacy conflicts and strategies of everyday life. The survey results particularly highlight the importance of mobile technologies with regards to privacy while simultaneously accentuating a lack of adequate strategies.

In light of this divergence, a qualitative study was designed to further explore the role of privacy in the context of mobile technologies. In a series of unstructured interviews with software developers this paper examines their privacy concept, knowledge of and experience with privacy measures as well as assessment of the different stakeholders involved in the debate around privacy.

Finally, the paper merges the findings of the theoretical and empirical work to create a design tool for professionals, focusing on those working in the field of mobile technologies.

2 PRIVATE SPHERES – STRUCTURING THE AMBIGUOUS

Firstly, the fluid, situational and ambiguous concept of privacy needs defining. An initial literature review reveals a scope of private spheres (Sloterdijk, 1998) that appears limitless: theoretically any facet of the self can be treated as private: a body, a behaviour, a thought, an interpersonal relation, a piece of information, a timeframe, a physical setting or an object (Nippert-Eng, 2007). Therefore this paper aims at classifying the hitherto diffusely delimited domain, proposing analytically and empirically verified information architectures, applicable to all design problems.

2.1 The Private Sphere – Characteristics of Interpersonally Negotiated Rules of Accessing the Self

Two millennia ago Plato defined privacy as the counterpart to the public sphere: the topic has been anchored in philosophical, sociological, political and anthropological discourse ever since (DeCew, Zalta, Nodelman, Allen, & Perry, 2009). However, no interdisciplinary, integrative definition of the scope of privacies has been agreed upon.

The theoretical groundwork to psychological types of privacy was given in Erving Altman's Privacy Regulation Theory (Altman, 1975), understanding privacy as a dialectic process of limiting/ allowing access to a person in an interactive situation. Prof. Anita L. Allen (1987) segmented privacy into the protection of physical, content-related and informational elements, distinguishing physical reclusion/ solitude (1), secrecy, concealment and data security (2), protection of a name, identity and the depiction of an individual in public (3). She completed this with the notion decisional privacy (Allen, 1999), adopted by scientists ever since (Pedersen, 2002). Alan Westin distinguished three privacy types, depicting attitudes towards privacy with regard to data security and informational protection, divided into privacy fundamentalists (1), privacy pragmatists (2) and privacy unconcerned (3) can be

found in his research findings (Westin, 2001). This extract of the analysis of the private sphere indicates the variety of theoretical models. Nevertheless no exhaustive, all-encompassing structure of privacy is offered: hence our motivation to approach the perception of privacy empirically through quantitative analysis, focusing on real-life examples of what's considered "private".

2.2 Empirical Approach – Quantitative Identification of Privacy Perceptions through Survey

In order to gauge how the public and private spheres are experienced, a quantitative survey was conducted to gather concrete interpretations. 197 respondents between the age of 16 and 63 were asked to name private/ public situations and conflicts. Furthermore, diverse implicit and explicit strategies to gain privacy in a public setting were inquired upon. The analysis was conducted via an online survey, all gathered example cases were clustered by topic and structured into three infographics: privacy perceptions (1), privacy/ public conflicts (2) and privacy strategies (3). This chapter highlights the first, linking practical privacy perceptions to the theoretical privacy structure derived from the previous literature review.

2.3 Proposed Model of Privacies – Segmentation and Visual Mapping

Literature and empirical analysis centers around one point: privacy is not a fixed and visible frontier between personal and public matters, but rather a flexible, permeable membrane of situational, selective accessibility - or lack thereof - to the self (Nippert-Eng,2007). This interactive negotiation of the protected elements of the self, versus the ones that are shared identifies the process of defining and delimiting privacy. Therefore, this paper uses the degree of interactivity to structure privacy:

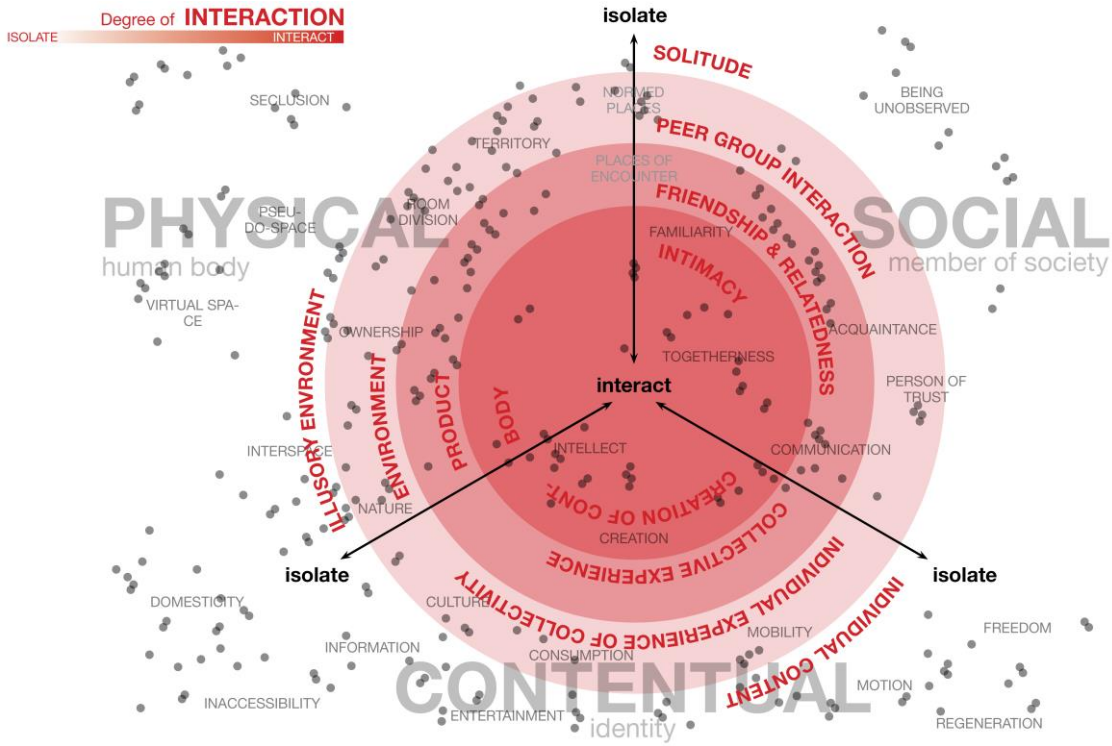

Figure 1. Degree of interaction structures privacies [own illustration]

The scientific research underlying this paper distinguishes three types of privacy: physical, social and contentual. Furthermore it proposes a concentric, layered structure to visualize four degrees of privacy: the relative distance towards the center ranges from maximal interaction (circle core, red) to maximal isolation (circle edges, white). Each dot is an empirically gathered answer to the question "name a situation in which you experience privacy". The dot distribution indicates that privacy can be perceived at any position in this structure, in situations of complete isolation and complete interaction. Thus this proposed information architecture distances itself from dialectic segmentations that attribute privacy to one of the poles, usually defining privacy as isolation and lack of interaction.

The public sphere is often considered the opposite pole to the private sphere (Sokol, 2001), (Brendgens, 2005). However, the clear edge between them has become blurred (Hitzler, 1985) and both notions appear intertwined: it is possible to experience privacy in public, and vice versa. Among the reasons for this blend, only a few are alluded to in this paper: the development of information and communication technologies allowing the public sphere to enter and be actively used to share formerly private situations, the digital revolution and shift towards virtual networks and marketplaces, logging our location, filming our behaviour in public, leaving a trail on the web (Harvard Symposium, 2011). Furthermore the understanding of collectivity and social groups has shifted away from the boundaries of a family to larger communities, changing the collective/ individual perception (Struppek, 2002) and the "sharing behaviour" of its members. Habits, linguistic expressions, customs and cultural codes have become less local, increasing connectivity with people from a variety of cultures and social backgrounds and reducing the frontier between an individual's private and public persona. All these elements lead to the potential for public/ private conflicts, which were analysed based on empirically gathered responses in the same online survey.

3 PRIVACY CONFLICTS AND STRATEGIES – MAPPING EXAMPLES

In the aforementioned survey, experienced challenges and solutions of the private and public sphere were further inquired upon.

3.1 Privacy Conflicts – Duality of Control between an Individual and their Surrounding

When asked to name conflicts of privacy/ public, the answers of 197 respondents can be grouped into two causal zones: privacy/public conflicts caused by a loss of control by the individual through the inability to protect one's privacy (1) and privacy/public conflicts caused be the privacy of others invading on an individual's privacy in public (2). This can furthermore be structured in the trichotomy of physical, social or contentual private/ public conflicts and mapped in an infographic (fig. 2).

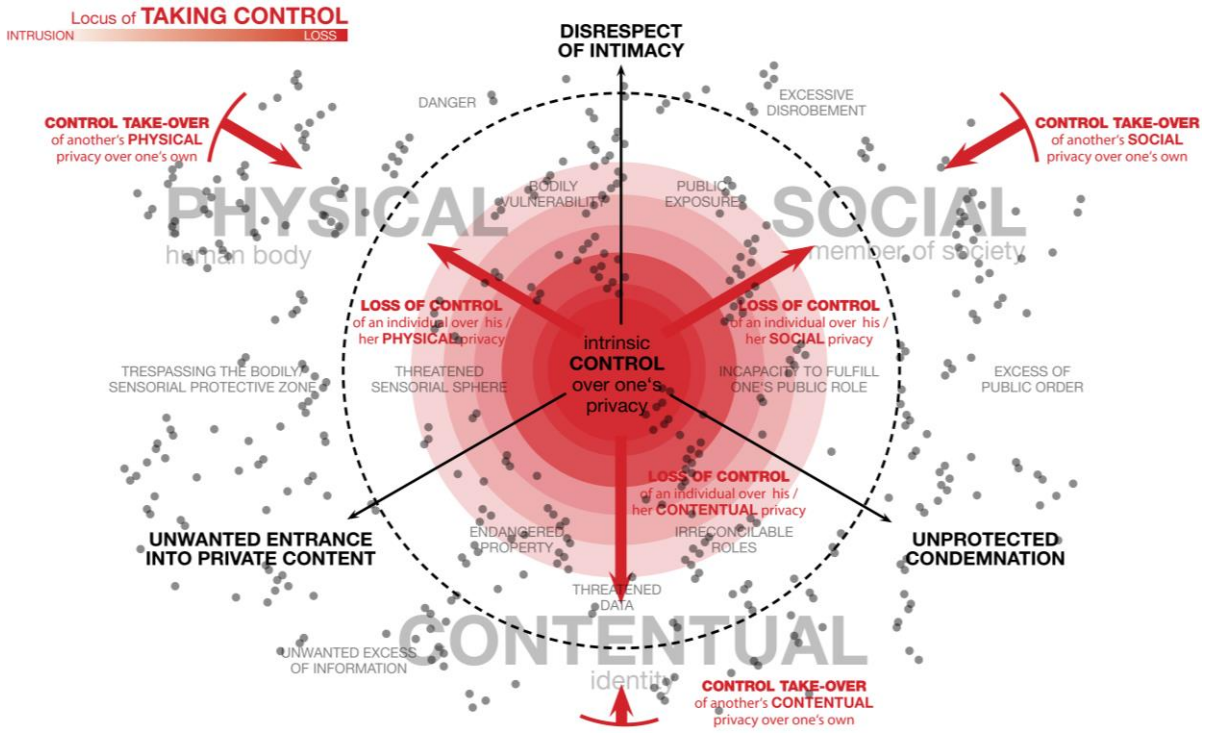

Figure 2. Duality of taking/ losing control structures privacy conflicts [own illustration]

What emerged from the analysis of privacy conflicts wasn't only the variety of situations in which the private and public spheres clash, but also the interesting frequency of occurrence of conflicts relating to the mobile technology sector.

3.2 Privacy Strategies – Methods to Acquire and Protect and Ephemeral Private Sphere in Public

Analogue to the previous analysis, clustering and mapping of conflicts, the empirical study yielded quantitative insights into strategies to acquire and preserve privacy in a public context. When asked "how do you generate/ protect your privacy in a public setting", the examples of all survey respondents can be structured according to their degree of initiative (proactive or reactive, x-axis) and degree of interaction (isolation versus interaction, y-axis), covering clusters of "adapting" (maximal reactive interaction) to "attack" (maximal proactive interaction), "cocooning" (maximal reactive isolation) and "evasion" (maximal proactive isolation).

Design is a crucial element to generate product and service solutions, in broader terms: shaping human experiences. Therefore any action geared towards creating privacy in a public setting can be defined as a design solution and placed along this structured by a dot (fig. 3). The diversity of possible privacy strategies emerges in this visual overview of the status quo of currently used strategies to create, communicate or defend one's privacy in the public eye:

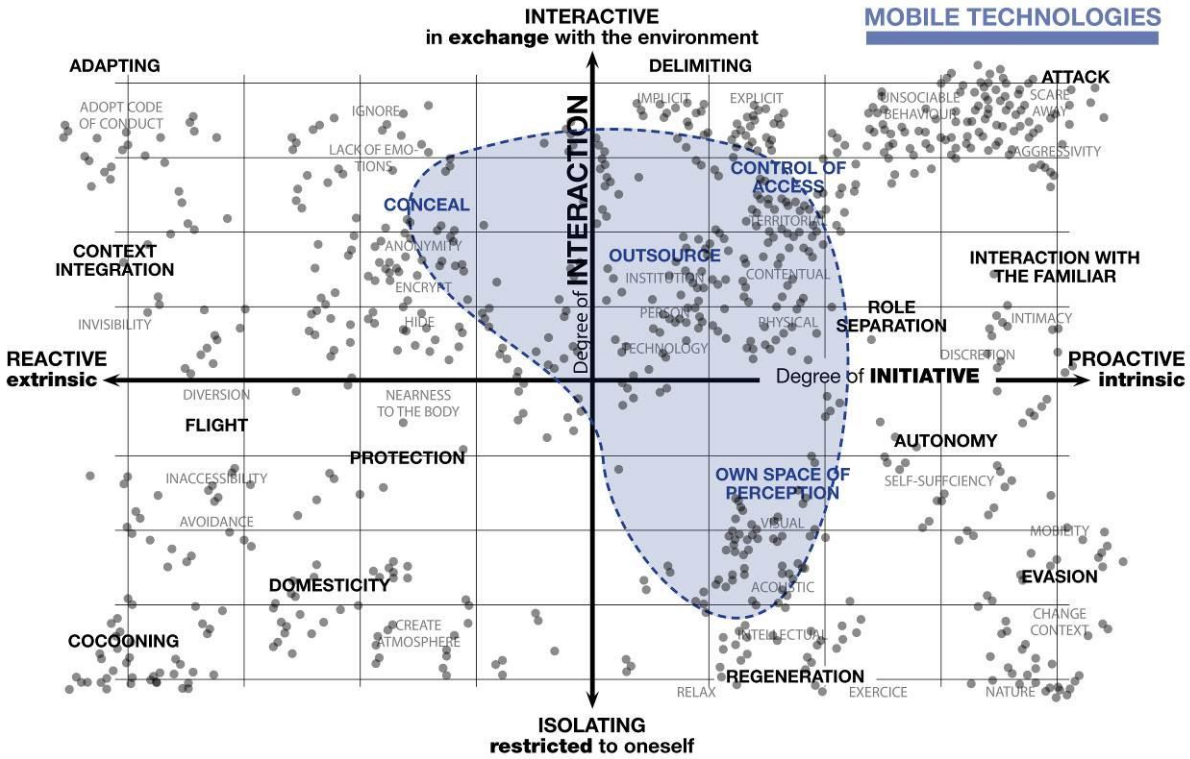

Figure 3. Cases of (re)gaining privacy by degree of initiative and interaction [own illustration]

The interesting discrepancy arising from the analysis of 3.1 and 3.2 is the high occurrence of mobile technology as a key privacy conflict, in light of the very limited field of privacy strategies that are currently used in the mobile technology – indicated in blue in fig. 3.

When viewing ubiquitous communication via mobile technologies as a metaphor for the public eye, this translates the decennia old privacy/ public conflict in our modern day and age: what are the implications of mobile technology on privacy and vice versa? Which privacy perceptions, conflicts and strategies given by *users* of mobile technology in the analogue world make sense in the mobile context and how is the issue currently approached by the other end of the spectrum: the people *developing* mobile technology solutions?

4 PRIVACY IN MOBILE TECHNOLOGIES – EXAMINING THE PERSPECTIVES OF MOBILE SOFTWARE DEVELOPERS

As illustrated in the previous chapter there is a jarring discrepancy between aspects that cause privacy conflicts in mobile technologies and strategies to obtain privacy, the latter being mostly physical, immediate interactions between humans. It is, however, still not clear whether strategies simply misfit the conflicts or whether the technology itself fails to offer adequate solutions.

While previous research has shed some light onto user concerns regarding privacy in a mobile context (Barkhuus and Dey, 2003), only little attention has been paid to the attitudes and practices of those who design and create the technological artifacts - mobile developers. To close this gap, this paper presents an empirical account for the privacy concept, conflicts and strategies within mobile software development from the perspective of developers.

4.1 Empirical Approach – Qualitative Investigation of Privacy through Unstructured Interviews

The qualitative part of this paper uses unstructured interviews as a means of data collection. The sample consists of 9 software developers, 8 males, 1 female.
All interviewees were self-employed, that is either working as a freelance developer or having founded their own company. Half of the participants were working either part- or full-time for clients that were not the end users themselves. Industries that the interviewees have worked in include as far as mentioned: health, education, event management, location-based services, media and entertainment. All interviews were digitally recorded, transcribed and analysed.
The qualitative analysis was software-aided and its theoretical background relies on the grounded theory method according to Strauss & Corbin (2008). Grounded theory is an approach to data analysis within which a theory is derived inductively from empirical phenomena. It involves an iterative, circular process consisting of data gathering, data analysis and theory construction.

4.2 Results – Privacy Concepts, Conflicts and Strategies from the Perspective of Mobile Developers

The data accumulated through the unstructured interviews was subjected to an inductive analysis. All insights presented are grounded in the qualitative data. They reflect the statements made by the interviewees and mirror their subjective understanding. Hence, the analytical details outlined below cannot be generalized to the whole population of software developers and represent only for sample referred to in this paper.

4.2.1 Privacy in Mobile Software Development – Three Dimensions of Informational Control

To explore the concept of privacy in the context of mobile technologies mobile developers were asked how they define privacy. Privacy was unanimously portrayed as the degree of control over information related to oneself, which also includes information about people one interacts with or is associated with. However, to have control over self-related information does not automatically equal privacy.
Control can refer to a multitude of things such as knowing what happens with self-related data or the amount and nature of third-party access to particular information, which can range from other single users or social groups to advertising companies. The degree of control depends on a variety of factors, which span three interdependent dimensions: social, technical and contextual. Those dimensions can be synthesized into a model that depicts privacy in a mobile context as the degree of control over information as outlined in figure 4.
What can be described as a continuum from interaction to isolation for the general concept of privacy is converted into a continuum of control and lack thereof. The level of control in one dimension will simultaneously affect control levels of the other dimensions.
The social dimension refers to aspects of identity of the self or others that one interacts with. Hence, a breach of privacy could be the possibility to tie a person's activities to their real identity or to track, collect, store and/ or share information about them.

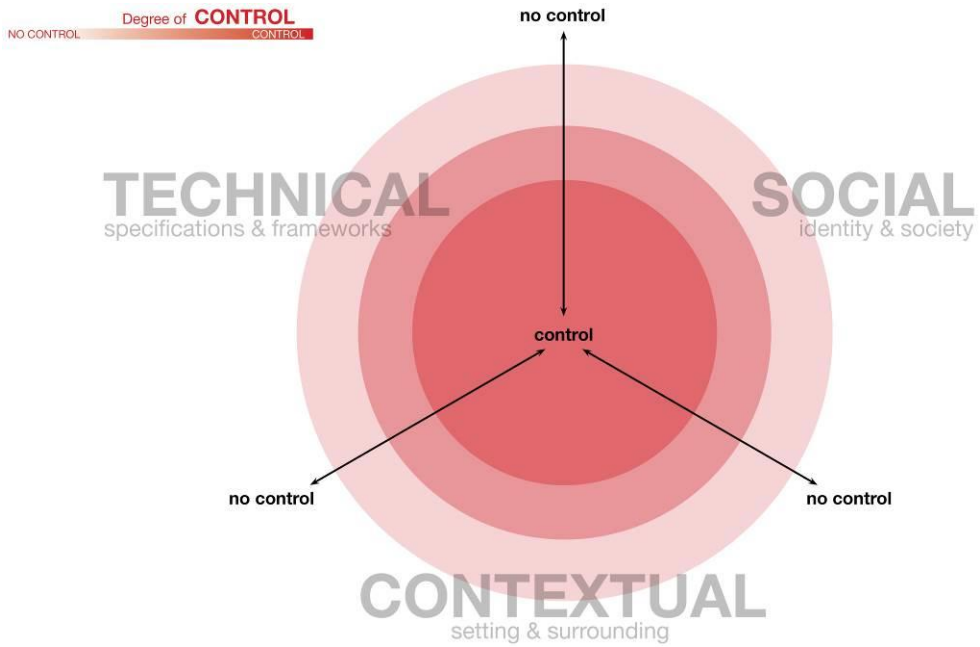

Figure 4. Control structures privacy in a mobile context [own illustration]

However, what is perceived as a violation of privacy in one context can be experienced as appropriate in yet another context, bringing the contextual dimension into play. A user might be happy to give away personal geo-location data, if in turn they are provided with a useful service. However, the analysis of personal correspondence for the same reason might be perceived as objectionable. In this case the context will determine the subjectively perceived degree of control and its relevance to the user.

Finally, the technical dimension, though somewhat peripheral to the construction of a privacy concept, bears tremendous influence on it. Technical aspects of an application can dictate whether or not the social details of a user are disclosed in any given context, making aspects such as consent and trust obsolete. Technology, though located on the outskirts of what constitutes privacy, penetrates to the very core of it by being able to take away the control from the user at any time.

All in all developers characterized privacy as an elusive, relative term. It is not an action or a particular state of being per se that defines privacy as warranted, but the affective, intraindividual evaluation of a person about what is appropriate and what is not. Moreover, in a mobile context this mental model is expanded by a technical dimension, which has enormous power over the degree of control.

Given this disproportionate influential distribution, technological aspects can be the cause of a plethora of privacy conflicts.

4.2.2 Privacy Conflicts – A Bipolar Continuum of Technical and Social Violations

As part of the interview developers were further questioned about privacy conflicts with regards to mobile technologies. They should describe conflicts that they were generally aware of, experienced themselves or have been confronted with by their users. A privacy conflict in the context of mobile technologies was defined as unwanted access to or distribution of information. Conflicts, then, are a violation of informational autonomy that results in undesired usage of information. Depending on the cause and type of violation conflicts can be positioned on a bipolar continuum between technical and social violations.

A technical violation is mostly economically motivated and associated with material loss. This can for example involve hacking an account and/ or gaining access to sensitive data, such as financial details or the tracking and selling of user specific information to another party, such as an advertising company. A social violation is associated with embarrassment and reputational damage. Access and distribution of sensitive information to other members of various social groups or the general public result in an aversive emotional state. This can for example include reading a personal message or using functions of a mobile application, such as a rating or review function, to share inappropriate information. Technical violations do not only require specific knowledge to access and distribute information, they also rely on the objective validity of that information. There is no use in erroneous

banking details or shopping preferences. Social violations, however, do not have to be genuine in nature to constitute a threat. Also, while technical violations are mostly consciously motivated by some material gain, social violations entail numerous motivations, which can be conscious or unconscious. A person can accidentally read a private message and thereby unknowingly violate someone's privacy. Likewise, a person can engage in punitive, malicious or derisive behaviour and deliberately access and spread information.
In the same way conflicts are continuously distributed between two poles, also privacy strategies can be positioned on a continuum between measures that are technologically-aided and measures that rely on proper conceptual design of an application.

4.2.3 Privacy Strategies – Acquiring Privacy through Technical and Conceptual Design

In light of the diverse causes of privacy conflicts, developers were subsequently asked to discuss strategies to prevent or resolve those conflicts. In particular they should assess the role of the user within the privacy debate as well as elaborate on strategies to protect privacy. Those strategies do not only include current actions and procedures, but also the assessment of future solutions to previously discussed conflicts. Developers expected users to be mindful and responsible with regards to the information they provide deliberately. However, they highlighted that technology ought to *enable* the user to fulfill those characteristics. Strategies depicted by the developers can be segmented in technical and conceptual strategies. Technical strategies refer to measures such as the encryption and secure storage of data, establishment of secure communication protocols as well as thorough data deletion and restriction of third-party access. Those strategies were viewed as straightforward and rather clearly defined. Conceptual strategies, however, were perceived to be more complex. They refer to all the interaction points with user and essentially touch upon the design of an application, which should make it easy for users to protect their data and share it responsibly. Conceptual strategies discussed by the developers included the adequate design of good and protective default settings. Further, transparency has to be established, that is, users need to be informed about changes in the system and its functionality as well as provided with explanations as to why certain permissions to their data are necessary. Moreover, a correct construction of language is essential, which will provide information in a clear and concise way.

5 DESIGN TOOL – DEVELOPMENT OF A BETA-VERSION TOOL FOR PRIVACY IN PUBLIC

The quantitative empirical research in this paper illustrated a complex layered, multidimensional model of privacy structured by degrees of interaction with most privacy conflicts occurring in the context of mobile technologies, but most strategies employed by users being inept in this context.
A qualitative analysis of the privacy concept in mobile software development revealed that although conflicts and strategies can be technology-related as well as technology-aided, most of them rely on user interaction and the design behind the technology to a very high degree.
Hence, this paper combines analogue user strategies of maintaining privacy with digital solutions from developers to create a design tool that will address this issue area. The design tool represents a user-generated, searchable database, which can be consulted via a website/ smart device application. It is comprised of cases that on the one hand communicate real-life privacy conflicts related to mobile technologies and on the other hand map them to user-generated design solutions.
The tool is meant to be a living document that is enriched by everyday experiences and paired with sophisticated, crowd-sourced solutions as to how to manage them.
The first working prototype is equipped with conflicts and respective solutions from the research outlined in this paper and will be augmented and substantiated by user-generated content. The tool provides a platform for design and engineering professionals to interact with their users as well as colleagues and enables them to solve existing or upcoming conflicts.

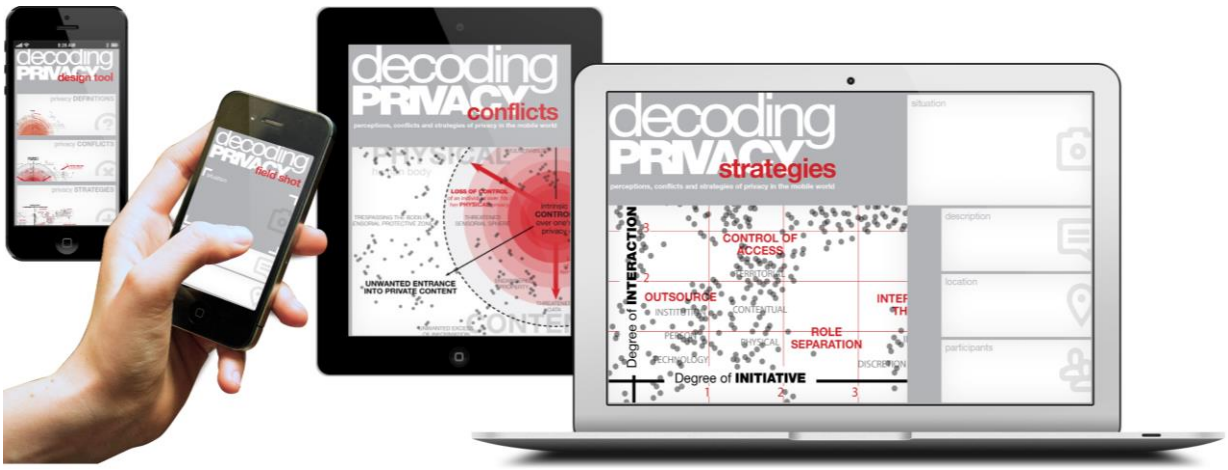

Figure 5 –Beta-Version of Design Tool mapping privacy perceptions, conflicts and strategies [own illustration]

6 CONCLUSION AND FUTURE OUTLOOK

This paper outlines the transdisciplinary theoretical and empirical analysis of privacies in the mobile technology context, resulting in a structural model of (1) perceptions of privacy, (2) the conflicts of privacy within ubiquity as well as mobile technologies, (3) the strategies to acquire and protect privacy and (4) the *decoding privacy* design tool, aimed at mobile developers and designers. By combining methods from design thinking, social sciences and product engineering, the design tool developed in this research positions design sciences at the core of solving one of future's most pressing challenges – *privacy in light of mobile technologies.*

The concluding design tool consolidates and visualizes all information and serves as guideline and case collection towards developing better product and service solutions in a variety of physical and virtual applications. It allows designers and developers with a design problem in the field of privacies/ ubiquity to position their specific case within the layers, thus clearly (re)defining their problem within the theoretical and empirical framework. Furthermore, neighbouring examples can be viewed, risks for similar conflicts assessed and a broad diversity of privacy solutions using multiple strategies evaluated. This Design Tool is currently in its beta phase, being tested by two design teams in Brussels and Munich and improved before going live, presumably late summer 2013. In its next phase, the design tool will allow accumulation of user-generated content: enabling users to learn from input, examples, insights and mistakes fellow designers or mobile developers have encountered.

Despite the theoretical and practical implications of this work it should be noted that future research is necessary to further explore some of the insights gained in this research. Though there is a strong negative correlation between privacy conflicts and currently used strategies, no definitive causal conclusions can be made. Additional investigations should address these aspects and specifically tie privacy strategies to the respective conflicts. Furthermore, the analysis of mobile developers' privacy concept is qualitative in nature and hence insights derived from this work are limited to the specific sample. Future research should explore whether the analytical results can be validated for developers from different cultures and industries.

ACKNOWLEDGEMENTS

Sincere Thanks to Sandra HIRSCH and Prof. Fritz FRENKLER at Technical University Munich, Lukas MURMANN, Miriam ALTHAMMER and Philipp WALZ for the urban privacy research in Munich and Johannes LECHNER and Albert FELLER for IT and coding support in building the Beta.

REFERENCES

Allen, A.L. (1987) 'Taking Liberties: Privacy, Private Choice and Social Contract Theory', *University of Cincinnati Law Review*, vol. 56, rev.461.

Allen, A.L. (1999) 'Coercing Privacy', *William and Mary Law Review*, vol.40, no.3, rev.723.

Altman, I. (1975) *The environment and social behaviour: privacy, personal space, territory, crowding*, Brooks/Cole Pub. Co.

Barkhuus, L. & Dey, A. (2003), 'Location-based services for mobile telephony: a study of users' privacy concerns', *Proceedings of the INTERACT 2003, 9TH IFIP TC13 International Conference on Human-Computer Interaction*, Zurich, September 1-5, pp.709-712.
Brandeis, L. and Warren, S. (1890) 'The Right to Privacy', *Harvard Law Review*, vol.4, no.5, pp.193-220.
Brendgens, G. (2005) 'Vom Verlust des öffentlichen Raumes - Simulierte Öffentlichkeit in Zeiten des Neoliberalismus', *UTOPIE kreativ*, pp.1088-1097.
DeCew, J., Zalta, E., Nodelman, U., Allen, C. and Perry, J. (2009), *Privacy*, Menlo Park, Stanford University, Center for the Study of Language and Information.
Harvard Symposium, (2011) 'Introduction', *Hyper-Public - A Harvard University Symposium on Designing Privacy and Public Space in the Connected World, Harvard University, June 9-10.*
Hitzler, R. (1985) 'Und Adam versteckte sich - Öffentlichkeit und Privatheit als subjektive Erfahrung', *Soziale Welt*, vol.36, no.4, pp. 503-518.
Hubeli, E. (2005), 'Von der Öffentlichkeit zu einem Universum von Teilöffentlichkeiten', in *5 Jahre Landesinitiative Städtebaukultur NRW*, Gelsenkirchen/Duesseldorf, pp.46-51[unpublished manuscript].
Nippert-Eng, C. (2007) 'Privacy in the United States: Some Implications for Design', *International Journal of Design*, vol.1, no.2, pp.1-10.
Pedersen, D. (2002) Model For Types of Privacy by Privacy Functions, Provo, Academic Press.
Schaar, P. (2009) *Das Ende der Privatsphäre: der Weg in die Überwachungsgesellschaft*, München, Bertelsmann.
Sloterdijk, P. (1998) *Sphären I - Blasen*, Mikrosphärologie, Frankfurt am Main, Suhrkamp.
Sokol, B. (2001) *Mediale (Selbst-)Darstellung und Datenschutz*, Duesseldorf, Landesbeauftragte fuer den Datenschutz Nordrhein-Westfalen.
Strauss, A. and Corbin, J. (2008), *Basics of qualitative research: Techniques and procedures for developing grounded theory*, Thousand Oaks, Sage Publications, Incorporated.
Struppek, M. (2002) *Title: Interaktionsfeld - öffentlicher Raum im Digitalen Zeitalter*, Dissertation, Kaiserslautern, Universitaet Kaiserslautern.
Turkle, S. (2004) 'How computers change the way we think', *Chronicle of Higher Education*: *Information Technology* [online], http://chronicle.com/article/How-Computers-Change-the-Way/10192/ (13.05.2013).
Westin, D. (2001) 'Balancing Privacy and Public Uses of Criminal History Information', in T. N. Statistics (Ed.) (2001), *National Conference on Privacy, Technology and Criminal Justice Information*, Sacramento, SEARCH, The National Consortium for Justice Information and Statistics, pp.38-46.