Addressing the Privacy Paradox by Expanded Privacy Awareness – The Example of Context-Aware Services

André Deuker

Goethe University Frankfurt
Chair of Mobile Business & Multilateral Security
D-60629 Frankfurt a.M., Germany
Andre.Deuker@m-chair.net

Abstract. When interacting with applications, users are less restrictive in disclosing their personal data than if asked in an application-independent context. On a more general level this behavior is termed as privacy paradox. The creation of privacy awareness can assist users in dealing with context-aware services without harming their privacy unintentionally, thereby addressing the privacy paradox. The paper in hand provides a research approach towards the integration of privacy awareness on an application-specific level, especially taking into account conflicting interests between users and providers of context-aware services. It shows that expanding privacy awareness towards knowledge about methods and tools to react turns out to be useful.

Keywords: Privacy Paradox, Privacy Awareness, Economics of Privacy, Context-Aware Services

1. Introduction

When thinking about the usage of context-aware services, many people may wonder what consequences it has to provide personal information to a (unknown) service provider[1]. Does the service provider process the information properly; in a way the user intends and expects him to? Does the information a user reveals in fact comply with what he wants to reveal, or is it possible to use disclosed information to convey additional information the user may want to keep private? On the other hand, the provision of personal information is often a necessity for the creation and provision of services and providing less, wrong, or inaccurate information could mean that the service is not performing in a way the user expects it to. One example is location based recommendations [12].

In reality fewer people care about such questions than one would expect, especially with regard to the associated risks of disclosing information imprudently [14]. Having a look at the privacy paradox, one has to admit that this might be not due to very relaxed attitudes towards privacy, but rather because of a lack of awareness with regard to which data is disclosed, and possible consequences a disclosure might bear. The goal of the research approach presented in this paper is to assist average

[1] A definition of the terms “context” and “context-awareness” can be found in [6].

individual users in dealing with context-aware applications without harming their privacy unintentionally. To build the theoretical basis, Chapters 2, 3, and 4 focus on the underlying theories of the privacy paradox, and on the creation of privacy awareness itself. Chapter 5 then builds on the insights of the previous chapters, and applies this knowledge on the creation of privacy awareness in context-aware services. Chapter 6 gives a summary of the article, states the scientific contribution, and opens the discussion for further research in this area.

2. The Privacy Paradox

Privacy economists are investigating users' trade-off between benefits and costs of disclosing personal information by means of utility functions for a number of years. The utility function of AWAD and KRISHNAN for instance derives benefits by the degree of the received service personalisation, whereas costs are influenced among other factors by consumers' privacy concerns [3]. To give an example: By providing personal information to a recommendation system as employed by Amazon.com, one could expect to benefit from better recommendations. On the other hand, this might be related to concerns with regard to the protection of the disclosed data, thus creating costs. The inherent assumption of this approach and economic approaches in general is that users seek to maximise their utility constantly by balancing costs and benefits.

Research on rationality in individual decision processes has shown that in principle people are quite clear and well able to articulate their desired level of privacy, at least on an abstract level. Nonetheless, having a look at their behaviour in privacy relevant decision scenarios, it has been observed that peoples' actual decisions do not correspond to their claims regarding their own privacy [2][14].

In literature this phenomenon is discussed as "Privacy Paradox" – human behaviour that does not correspond to the behaviour one could expect given the articulated attitudes towards privacy [9].

Although the existence of the privacy paradox seems to be evident, and might be underlined by personal experiences of many readers, the following section attempts to show that the underlying mechanisms responsible for the paradox are manifold, hard to catch, and even harder to combine within one meta-theory.

3. Three Dimensions of the Privacy Paradox

Research has been performed in order to understand reasons and draw connections to existing theories of human behaviour. Within this article, emphasis is put on three different approaches that can be found in literature. The approaches are motivated by [2]. They correspond well with each other, give explanations on different aspects of the paradox, and can thus be termed as dimensions of the privacy paradox. Further dimensions may exist.

The first two dimensions, the state of *incomplete information* and *bounded rationality*, are commonly used in economic theory. Homo Oeconomicus – the economic prototype of an individual – constantly seeks to maximise his benefits by

making rational decisions, whereas the decisions are based on the information he has and he can process. Objectively irrational decisions and actions (as in case of the privacy paradox) can be explained by individuals' limited capabilities in accessing and processing decision relevant information. Although objectively irrational, the behaviour of individuals is considered to be subjectively rational within the given boundaries of perception.

With regard to the limitations in accessing information essential for an objective decision on privacy matters, two facets of incomplete information are worth to be considered:

- **Incomplete information about disclosed data:** Users may not be aware of data they disclose. This refers to a situation in which users' behaviour is observed, stored, and processed without their knowledge. Thus, risks arising from this cannot be considered.
- **Incomplete information about consequences of disclosed data:** Disclosing some information explicitly does not mean that only this information is available to others. Additional information might be derived e.g. by linking the disclosed data with other sources of data. Information the individual wants to keep private might be derived. In a profiling challenge, students were able to capture the Wikipedia user-pseudonym the target person used in his business life. As the target person was very active in Wikipedia the students were able to derive an approximation on working hours and the potential periods of holidays within the last two years by analysing dates and times of entries in forums and contributions to articles[2].

Incomplete information can be considered to explain at least one part of the privacy paradox; but also considering a world in which every piece of decision relevant information is accessible to the user, the vast amount of information available itself would constitute a problem.

- **Bounded rationality results in wrong or biased conclusions:** As described by SIMON in the concept of bounded rationality [13], users' capabilities in processing information and drawing the right conclusions are restricted by nature. This can e.g. result in an over- or underestimation of risks associated with the disclosure of data. The approach of bounded rationality is a concept often considered in theories of human behaviour in the context of new media and services [15].

Beside these two more economic driven theories, *psychological variables* also contribute to give explanations for the privacy paradox. Having a look in psychological literature, one can find detailed research results describing individuals' attitudes towards benefits, costs, and risks in different horizons of time.

- **Users draw less attention to privacy risks than to other types of risk:** BREHM differentiated between different types of risk and their meaning for individuals. Threats that rise within a horizon of time (e.g. threats to privacy) are considered to be less important than immediately arising threats. Threats

[2] The profiling challenge took place as part of the information and communication security course at University Frankfurt in winter term 2007/2008. The exercise was inspired and based on a similar exercise within the 2005 FIDIS PhD Consortium (www.fidis.net).

that can be mitigated by personal behaviour (e.g. threats to privacy) are considered to be less important than threats users are exposed to passively [5].

- **Immediate gratification can influence users' (privacy) risk perception:** The presence of immediate gratification can affect users' perception of potential future threats [1]. Thus, privacy risks are likely to be underestimated in the presence of immediate beneficial incentives.

When striving for the best possible explanation, the above-mentioned factors need to be considered as well. Beyond previously mentioned dimensions further factors may influence individuals' behaviour in privacy relevant decision scenarios. Examples are group pressure in social networks or the impact of media and society in general.

4. Privacy Awareness

When aiming to resolve the privacy paradox it makes sense to reflect on how dimensions as incomplete information, bounded rationality, and various psychological factors can be addressed. This may be easier and more successful within concrete privacy sensitive applications. With regard to the aspects of incomplete information and bounded rationality, it seems to be very clear that individuals need to be supported with regard to the collection and processing of their personal data. As an initial step, awareness has to be created or raised in order to motivate individuals to take care of this problem. In this chapter we understand privacy awareness as individual users' ability to identify and assess risks associated to the disclosure of personal information. This approach will be extended in chapter 5.

4.1 A Precondition for the Employment of PETs

Several methods and technologies have been developed in order to mitigate risks that are connected to the disclosure of personal data. Within the domain of computer science and related fields, concepts and implementations for systems supporting anonymity, pseudonymity, unlinkability, or untracability, were developed. Other disciplines may contribute to support users in protecting their privacy as well. Nonetheless, applying privacy enhancing techniques in a reasonable way requires users initially to be aware of the problem's dimensions or of the existence of the problem at all. To give an example: Privacy Enhancing Technologies (PETs) are well able to cope with certain threats, but:

- If users are not able to identify risks, they will not get the idea to employ PETs.
- If users are aware of risks only on a very general level, they might want to take countermeasures, but they will not be able to assess whether costs for embodying PETs are justified.

Being aware of risks associated with the disclosure of personal data is the precondition to deal with them in an appropriate and rational manner.

Raising privacy awareness is thus a first and essential step for motivating individuals to reflect on privacy issues in concrete usage scenarios. Privacy awareness

can be raised in different contexts and in different fashions. A valuable segmentation of dimensions of privacy awareness has been provided by PÖTZSCH distinguishing between user-independent vs. user-specific, and application-independent vs. application-specific privacy awareness [10]. In the following, emphasis is put on the application-specific dimension of privacy awareness; in particular on the integration of privacy awareness raising mechanisms in context-aware services. Moreover, the concept of privacy awareness is expanded from awareness of problems towards awareness of possible solutions, as a means to overcome the privacy paradox.

4.2 Privacy Awareness on an Application Level

Privacy awareness in context-aware services can be raised by different means. On a general level privacy disclaimers can contribute to mitigate the effects of users' incomplete information on what is going to be done with their data. The effectiveness of privacy disclaimers with regard to raising privacy awareness is nonetheless questionable, and suffers from the extensive amount of information that comes with them. Because of bounded rationality, users are not able or willing to appreciate this information. As privacy risks are systematically underestimated, described in chapter 3, users will probably not even get the idea to employ advisory tools as e.g. privacy bird [11] to overcome bounded rationality. On a situation specific level, privacy awareness can be raised directly before the actual disclosure of personal data. This has the advantage that the properties of the specific type of information that is going to be disclosed, can be taken into account. Research on how to implement privacy awareness on a situation specific level is still in its infancy. First approaches can be found in related research areas: Within a study on transparent mobile recommendation systems, design criteria have been developed on how users can be supported in understanding what personal information has influenced the actual recommendation [12].

5. Towards a Research Approach

The previous chapters laid out the theoretical ground for an initial research approach that is presented within this section. Following, the problem domain of the research approach is outlined and hypotheses are derived. The chapter closes with an outlook on the application of the design science paradigm that is going to be used to address and probe the hypotheses.

5.1 Problem Domain: Establishment of Application-Specific Privacy Awareness

The motivation of this research approach is to contribute to the establishment of privacy awareness on an application-specific level of context-aware services. "Average" users that are not aware of pitfalls related to the disclosure of personal information in context-aware services should be enabled to assess risks more

objectively. Thereby the discrepancy between actual and desired behaviour should be reduced.

Different challenges arise when it comes to the establishment of mechanisms contributing to raise users' privacy on an application-specific level. Beside the questions on how these mechanisms have to be designed and integrated in the processes on a technical basis, it needs to be considered which parties are involved in this process.

In contrast to the establishment of privacy awareness on an application-independent level, e.g. by tutorials and exercises as in the above-mentioned profiling challenge, different parties and their interests have to be considered and harmonised when striving for privacy awareness on an application-specific level. Most important parties in this process are service provider and user of context-aware services.

Knowledge about users' identity attributes is crucial and an essential asset for every provider of context-aware services. It determines the degree of personalisation that can be achieved and thus the quality and price that can be charged for the service. This holds true for different types of context-aware services, among of them mobile services based on location information, e.g. mobile recommendation systems, mobile social communities or services based on individualised mobile advertising.

In principle there are two ways how privacy awareness can be established on an application-specific level. On the one hand, the legislator might oblige providers of context-aware services to establish privacy awareness enhancing mechanisms. This can easily run into a very complex process, as it is not clear whether a one-fits-all regulation is appropriate to address the issue. On the other hand, economic incentives can motivate providers to spend money on raising privacy awareness.

At first glance there seem to be no economic incentives for providers to invest in privacy awareness. On the contrary, disadvantages seem to be predominant: Research on the impact of consumers' privacy concerns gives indications that users will be more likely to provide less, or incomplete information when their concerns with regard to the protection of their privacy rise [8]. This is also underlined and even amplified by the psychological effect of reactance, an emotional overreaction with regard to a presented threat, risk, or confinement of alternatives [5]. As a consequence, users are even likely to disclose less information than with a neutral perspective. Raising privacy awareness in a sense of raising consumers' concerns thwarts providers' attempts to collect as much data as possible for the process of personalisation. How to overcome this?

5.2 Expanded Privacy Awareness: A Means to Address the Privacy Paradox on an Application-Specific Level

The Theory of Psychological Reactance by BREHM states that users will attempt to regain the threatened freedom, in this case their privacy, by whatever method available [5]. If users are not enabled to disclose personal data while preserving their privacy, it can be assumed according to [8], that they will indeed provide less information or even completely abstain from providing information; as this is the only method to regain the threatened freedom. Therefore we propose:

P1: To overcome the privacy paradox, raising privacy awareness on an application-specific level should be closely connected with raising knowledge about methods and tools essential to satisfy needs with regard to the protection of privacy in a meaningful way.

By this proposition we expand the meaning of privacy awareness from awareness of problems towards awareness of possible solutions as a means to overcome the privacy paradox.
In addition to P1 we propose that raising privacy awareness on the one hand, and providing means that allow users to react on their needs with regard to the protection of privacy on the other hand, positively affects the relation between user and provider of a service.

P2: Raising privacy awareness in connection with providing privacy enhancing technologies on an application level can strengthen the relationship between user and provider of a context-aware service.

This constitutes an economic incentive for providers to accept or even support the creation of privacy awareness within their applications. Focussing on potential incentives that could motivate providers to enforce the creation of privacy awareness, the goal of the research approach is to assess whether a combined approach of enhancing privacy awareness on the one hand, and providing privacy enhancing means on the other hand, can motivate customers to provide more or more accurate personal data than before. This is reflected in Proposition 3.

P3: The combined approach of raising privacy awareness and providing means to react will result in more or more accurate disclosed personal data.

The Propositions P1, P2 and P3 are based on a literature review on the underlying theories of the privacy paradox, as well as on privacy awareness and related topics.

5.3 Outlook: Applying the Design Science Paradigm

Research on information systems (IS) is still young compared to related disciplines of computer science and economics. Methods to address problems in IS research are not confined to a traditional and established set of alternatives. This, among other factors, led to a discussion on the discipline's identity [4]. Nonetheless, on an abstract level the paradigms of behavioural-science and design science exposed to be predominant for research in IS [16]. The focus of behavioural-science is on the discovery of truth to explain or predict human or organisational behaviour. Design science seeks to discover artefacts that proactively address relevant problems in the area of IS. Design science is inherently a problem solving process, whereas a problem is defined as discrepancy between a goal state and the current state of a system [7].

Several theories from the area of behavioural-science were used within Chapters 2 to 4 to derive and underline the problem description laid out in Chapter 5.1. In future

research, the propositions derived in Chapter 5.2 will be addressed, substantiated and evaluated mainly by following the design science paradigm.

The article in hand derives a problem description and gives substantiated evidence for the problem's relevance. A first rudimentary version of an artefact was proposed by describing a method on how to integrate privacy awareness on an application-specific level[3]. In a next step the insights of this paper will be embedded into the design science framework provided by HEVNER [7] to allow for a proper enhancement of propositions, e.g. to consider the heterogeneity of user in the process of awareness creation, and to derive provable hypotheses. The author plans to create a context sensitive mobile application to implement privacy awareness in a way as described in Proposition 1. Following up on this the hypotheses should be validated by an experimental comparison against already existing, less privacy focussed, context-aware mobile applications.

6. Summary and Concluding Remarks

Within this paper a research approach in the area of privacy in context-aware services was presented. Based on a literature review the phenomenon of the privacy paradox has been described and explanations were given by referring to economic and psychological theories.

Based on the theoretical ground laid out in chapters 2, 3, and 4, chapter 5 particularly addressed the establishment of privacy awareness on an application-specific level. In contrast to the application-independent creation of privacy awareness, interests and perspectives of more involved partners need to be considered when creating privacy awareness on an application-specific level, as e.g. in context-aware services.

It has been shown, that raising privacy awareness alone can result in a conflict of interest between users and providers of services, as users might disclose less of their personal information than before. In contrast to that, it was proposed that combining the creation of privacy awareness with tools that allow users to react in a meaningful way can end up in a win-win situation. By these propositions we expand the meaning of privacy awareness, from awareness of problems, towards awareness of possible solutions as a means to overcome the privacy paradox.

Acknowledgements

I would like to thank Prof. Kai Rannenberg and my colleagues at the Chair of Mobile Business & Multilateral Security for many helpful discussions and inspirations. In addition to that I received many valuable comments in the course of the PrimeLife Summer School and during the final review.

[3] In the context of the design science framework by HEVNER [7] this can be classified as a contribution to Guideline 1 (Design as an Artifact) and Guideline 2 (Problem Relevance).

The research leading to this results was supported by the European Union Projects Future of Identity in the Information Society (FIDIS, project number 507512, www.fidis.net), PrivacyOS (project number 225044, www.privacyos.eu) and the German Federal Research Ministry project PREMIUM-Services (project number 01|A08003C, www.premium-services-projekt.de/).

References

1. Acquisti, A.: Privacy in electronic commerce and the economics of immediate gratification. In Proceedings of the 2004 ACM Electronic Commerce Conference (2004)
2. Acquisti, A., Grossklags, J.: Privacy and rationality in individual decision making. In: IEEE Security and Privacy, vol. 3, no. 1, pp. 26-33 (2005)
3. Awad, N. F., Krishnan, M. S.: The personalization privacy paradox: An empirical evaluation of information transparency and willingness to be profiled online for personalalization. In: MIS Quaterly, vol. 30, no. 1, pp. 13-28 (2006)
4. Benbasat, I., Zmud, R. W.: The Identity Crisis within the IS Discipline: Defining and Communicating the Discipline's Core Properties. In: MIS Quarterly 27, 2, pp. 183-194 (2003)
5. Brehm, J.: A Theory of Psychological Reactance. In: Festinger, L., Schachter, S. (eds.): Social Psychology. A series of monographs, treatises, and texts. Academic Press, London (1966)
6. Dey, A. K., Abowd, G. D.: Towards a Better Understanding of Context and Context-Awareness. In: CHI 2000 Workshop on the What, Who, Where, When, and How of Context-Awareness (2000)
7. Hevner, A.R., March, S.T., Park, J. et al.: Design Science in Information Systems Research. In: MIS Quarterly 28, 1, pp. 75-105 (2004)
8. Hoy, M.: Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concern. In: Journal of Advertising, 28, 3, pp. 41-45 (1999)
9. Norberg, P. A.; Horne, D. R.; Horne, D. A.: The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. In: Journal of Consumer Affairs 41, 1, pp. 100-126 (2007)
10. Pötzsch, S.: Privacy Awareness – A Means to Solve the Privacy Paradox? In: V. Matyáš et al. (Eds.): The Future of Identity, IFIP AICT 298, pp. 226–236, 2009.
11. Privacy Bird Website: www.privacybird.org (accessed on 2009-07-22)
12. Radmacher, M.: Design Criteria for Transparent Mobile Event Recommendations. In: Proceedings of the 11th Americas Conference on Information Systems, Toronto (2008)
13. Simon, H. A.: Models of bounded rationality. Cambridge, MA: MIT Press (1982)
14. Spiekermann, S., Grossklags, J., and Berendt, B.: E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In: Proceedings of the 3rd ACM Conference on Electronic Commerce, pp. 28-47, New York (2001)
15. Zerdick, A., Picot, A., Schrape, A.: Die Internet-Ökonomie: Strategien für die digitale Wirtschaft. European Communication Council Report, Springer, Berlin (2006)
16. Zmud R.W.: Editor's Comments. In: MIS Quaterly 21, 2, pp. xxi-xxii (1997)