Privacy Awareness - A Means to Solve the Privacy Paradox?

Stefanie Pötzsch

Technische Universität Dresden[1]
Faculty of Computer Science
D-01062 Dresden, Germany
stefanie.poetzsch@tu-dresden.de

Abstract. People are limited in their resources, i.e. they have limited memory capabilities, cannot pay attention to too many things at the same time, and forget much information after a while; computers do not suffer from these limitations. Thus, revealing personal data in electronic communication environments and being completely unaware of the impact of privacy might cause a lot of privacy issues later. Even if people are privacy aware in general, the so-called privacy paradox shows that they do not behave according to their stated attitudes. This paper discusses explanations for the existing dichotomy between the intentions of people towards disclosure of personal data and their behaviour. We present requirements on tools for privacy-awareness support in order to counteract the privacy paradox.

Keywords: Privacy, Privacy Awareness, Privacy Paradox

1 Introduction

The protection of privacy is an important issue in modern information society. The release of personal information in electronic communication environments may cause severe privacy issues in the future, if people are completely unaware of their privacy. Secondary uses of data promote these problems further 22. Even if people have a theoretical interest in keeping their privacy when acting on the Internet and do not want everybody to know their personal data and private information, studying their real online communication often shows a different behaviour. This seems to be a paradox.

In this paper we present an approach for how the privacy paradox can be addressed. Therefore options for supporting awareness of privacy by technical means are discussed and requirements on these tools are outlined.

The structure of the paper is as follows. In Section 2, we briefly summarise two understandings of privacy which are relevant in the scope of interactive applications on the Internet, and based on that definitions we introduce our concept of privacy

[1] The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 216483.

awareness. In Section 3 we present studies about the attitudes of people towards privacy and their actual behaviour and we discuss potential reasons for the dichotomy between both. Objectives and requirements for technical tools to support privacy awareness are outlined in Section 4. We conclude the paper in Section 5 and indicate directions for further research.

2 Privacy Awareness of People

The term privacy awareness is not well established in the literature. Hence, as a starting point, we present interpretations of privacy, which are taken into consideration for this work. After the concept of awareness is introduced, we give a definition of privacy awareness.

2.1 Privacy

Various meanings and dimensions of privacy have been discussed in literature (e.g. 3, 7, 15, 16). Instead of going into detail on all these concepts, only two viewpoints are presented here, which are most important when discussing privacy awareness for interactive applications such as e-Commerce scenarios or Web communities. The two viewpoints are the privacy of personal sphere and the privacy of personal data.

- **Privacy of personal sphere**
  Samuel Warren and Louis Brandeis published the influential paper "The Right to Privacy" in 1890 and defined privacy as "the right to be let alone" 23. In this regard, privacy is understood as solitude and non-intrusion. It refers to (a) the secrecy of an individual's own thoughts, properties and actions and (b) the amount of data about others which flows towards the individual and possibly interrupt him/her 5. In everyday life, this kind of privacy is respected due to well-established social norms. People are easily able to understand whether they are in an open-plan office with several colleagues around or if they are in a mountain shelter with nothing other than green grass and stones surrounding them. In the first case it is obvious that documents, which lie on a table, may be noticed - intentionally or unintentionally - by others and that colleagues at any time may interrupt the work of the individual.

- **Privacy of personal data**
  Another view on privacy, often applied by computer scientists and labelled as information privacy, refers to "the right to select what personal information about me is known to what people" 24. This definition stresses the aspect of control over information about the individual, his/her conversations and his/her actions. The disclosure of personal data is bound to the recipient and to the usage and, in contrast to the concept of solitude, actively determined by the individual as owner of the data. To be able to select which data to disclose to whom, does not only

comprise options to keep data confidential but also options to disclose data to selected receivers, e.g. through the availability of communication means.

Comparing these interpretations, it is to say that the first one considers especially social aspects of privacy, whereas the second definition is more focussed on the data and therefore technical-oriented. Both views need to be taken into account when solutions that support privacy of individuals in technically mediated interactions with each other should be designed.

2.2 Privacy Awareness

Awareness is based on an individual's attention, perception and cognition of physical as well as non-physical objects. The state of being aware of something fades away as soon as there is no longer any stimulus present. Information from the environment or from other people constitutes such stimuli. Since the focus of this paper lies on privacy in the context of interactive scenarios between customers and service providers as well as collaborative use cases, where arbitrary entities interact with each other, the privacy awareness of people will be discussed.

Taking into account the two views on privacy presented above, privacy awareness of an individual encompasses the attention, perception and cognition of:

- *whether* others receive or have received personal information about him/her, his/her presence and activities,
- *which* personal information others receive or have received in detail,
- *how* these pieces of information are or may be *processed* and *used*, and
- *what amount* of information about the presence and activities of others might reach and/or interrupt the individual.

There are two main parameters for content and representation of information that serves as a stimulus for privacy awareness: the individual and the application. On the one hand, privacy-awareness information are of general nature, i.e., independent from individual preferences and independent from a particular application. On the other hand, privacy-awareness information are geared personally to an individual or to a specific application. These different dimensions of privacy-awareness information can be found in **Table 1** and are described below.

- **User-independent vs. User-specific privacy-awareness information**
  Means to build up and enhance privacy awareness can be identical for each user of a system or be tailored to group-specific or even to individual requirements and needs. Whereas privacy disclaimers on Websites can be seen as an example of general, user-independent privacy-awareness hints, the evaluation of individual privacy preferences can serve as a basis for more individualised and user-specific features of privacy-awareness support.

- **Application-independent vs. Application-specific privacy-awareness information**
  A broad spectrum of possibilities exists for raising the awareness of people for privacy issues and sensitising them towards their own personal privacy – in terms of personal sphere as well as in terms of personal data. On the one end of the spectrum privacy-awareness information is of general nature, i.e., independent from any special use case. On the other end, information regarding privacy is tailored towards a specific application.
  Talks, privacy campaigns or tutorials, e.g. the PRIME General Public Tutorial 18, are various means of providing application-independent privacy-awareness information. In such cases, the wish of people to be informed is necessarily required. They actively need to access the tutorial, attend the talk or read the campaign and afterwards apply their gained application-independent privacy awareness in concrete use cases, when they act within specific applications. Additionally, the application might have its own features for privacy awareness integrated and thus provide information which fits well in the current situation and privacy issues that may arise within the specific application. Obviously, intermediate levels and combinations between application-independent and application-specific information for privacy awareness exist and are necessary to support privacy awareness of people comprehensively.

Table 1. Dimensions of Privacy-Awareness Information

	User-independent	User-specific
Application-independent	*Talks, Campaigns, Tutorials*	*Individual advice from a Privacy Commissioner*
Application-specific	*Privacy Disclaimers on Websites*	*Feedback from Website's policy evaluation (e.g. Privacy Bird)*

3 The Privacy Paradox

Privacy awareness enables people to make informed decisions and should lead to less unintentional privacy-invasive behaviour. Consequently, it can be assumed that people who are conscious about privacy issues and state the intention to protect their personal data and their personal sphere, i.e., who can be considered privacy-aware, will act according to their statements if the have the choice between different options for action. However, several studies show a contradictory finding and are outlined in the next section. We discuss reasons for the observed phenomenon considering an economic approach to explain the behaviour first and the misconception of recipients of information second.

3.1 Studies about Intentions and Behaviour

An online shopping experiment compared self-reported privacy preferences of people with their actual self-disclosing behaviour and found out that a majority of the test participants – regardless of their previously stated privacy attitudes – disclosed a large amount of personal information 21. Similar results are shown in another study about intentions and behaviours of people towards privacy 17. The participants provided significantly more personal data than they claimed beforehand. Within this study the researchers also tested whether the perception of risks is more salient and has a negative influence on the stated intentions of people when they are asked in general, whereas this is not the case in real situations when they decide to disclose data. This hypothesis was supported by the results of the study. A further study was conducted in order to test the ratio between people's value for personalisation and their concern for privacy 6. A core finding from this research indicates that the value of personalisation is nearly two times more influential in the actual decision to use personalisation services and therefore to disclose personal data than the concern for privacy. This result shows that, even if people may be privacy-aware in general, they need to be at least two times more aware of privacy than of the benefits which they can gain from personalisation in order to make a balanced decision about whether personal data to disclose and which.

The contradiction between attitudes towards privacy and actual behaviour, identified in all of the cited studies, is called the *privacy paradox* 17. It would be of further interest to investigate the existence of this phenomenon in Web communities. First results of Acquisti and Gross 1 in this field indicate that a share of privacy-concerned people simply does not join in online social networks, which is not surprising. However, privacy-concerned people who are members of an online social network, share nearly the same amount of personal data (e.g. birth date, sexual orientation or personal address) as other members of the network. This indicates the existence of the privacy paradox in online social networking applications.

3.2 Balancing Values

When searching for explanations for the privacy paradox, the appreciation of values seems to play an important role.

The balancing of benefits and costs can be described by a utility function 4:

$$U(X) = \text{Benefit} - \text{Cost} \quad (1)$$

On the one hand, there are several benefits resulting from the disclosure of personal information in specific situations. On the other hand, people have their attitudes and evaluation of privacy, which can be seen as costs of disclosure. **Table 2** presents arguments for both perspectives. This occurs first in eCommerce situations as an example of a traditional customer-service provider orientated approach and, second, in Web communities which illustrate interactions among arbitrary individuals.

Table 2. Benefits and Costs for Disclosure of Personal Data

	Benefits	Costs
eCommerce	– Convenience – Automated processes – Price premiums – Selected information	– Price discrimination – Marketing spam – Identity theft
Web Communities	– Social exchange – Relationships – Collaborations – Reputation	– Identity theft – Marketing spam – Stalking, Kidnapping – Negative reputation in other contexts

If people are asked in general about privacy, and not in a specific situation, many of them are to some extent privacy-aware, as the cited studies show. However in real situations the concrete value of privacy (*costs*) is hard to estimate and is no longer salient to people. The quantity of possible price premiums or the "universe of new friends" (*benefits*) is primarily advertised; it is just a few clicks and disclosure of a few personal data items away. It is assumed that the privacy awareness of people in such situations is low, since there is a lack of stimuli at the moment of attention. The previously summarised studies support this hypothesis for eCommerce scenarios. With regard to the handling of personal data of members in social networks, this seems to be valid for Web community scenarios, too (10, 1), although the type of benefits and costs differ slightly. Web communities offer primarily social contacts, easy ways to find new friends, business cooperation, and so on. Since profiles of Community members are accessible for a lot of people on the Internet, identity theft in these cases is possible without great efforts. The risks of becoming a victim of crimes, which are based on personal information, or getting bad reputation in other contexts are costs of the disclosure of personal data which are discussed in the media from time to time. However, such issues do not appear to be salient to people in special situations when they interact within a Web community.

3.3 Misconception of Recipients

People are less concerned about their privacy if they have established relationships with other entities who are the perceived recipients 19. This causes additional privacy issues especially in Web communities, when members simply do not realise or "forget" that they potentially share personal information not only with some friends or a small group of forum members, but with a quiet mass of all Internet users who may have access to the social network or read their postings about their private life on public bulletin boards.

For conducting a study on "social phishing", researchers have used freely accessible profile data from a social network 12. After completion, the researchers explained the experiment on a Website and provided a public forum for anonymous discussion among the groups of victims and their friends. From this feedback it can be learnt that many of the subjects simply did not understand how information about them and their relationships were obtained. They believed that data on the social network is not public and is only accessible to their friends. However, it was not clear to them that anyone on the Web had access to their profiles and can snoop around in personal information. This fact illustrates the privacy paradox in terms of Web communities, since people obviously do not want everybody to have access to their private data. However, they publish this information on online social networks and do not realise that they provide their names, hobbies, phone numbers, addresses etc. not only to their friends, but to a broad public on the Internet.

4 Tools to Support Privacy Awareness

In principle, there exist two options to encounter the privacy paradox: either the behaviour of people would have to be adapted with their attitudes or vice versa. In order to enhance privacy, the first option should be pursued, i.e., people should be "reminded" about their intentions to protect privacy during interactions. Therefore tools and features need to be designed and developed that increase privacy awareness in specific software applications.

4.1 Objectives of Tools to Support Privacy Awareness

Privacy awareness is important for people in order to make informed decisions about the disclosure of data and to control the amount of possible interruptions during their work. Whereas the data disclosure refers to information privacy as defined previously, the consideration of possible interruptions caused by other parties is related to the notion of privacy as personal sphere.

It is usually incumbent on the users of applications not to forget their values of privacy whereas the scaling pan with the benefits for disclosure of personal data is advertised by providers of services and appears obvious in software applications. Tools for privacy-awareness support should help to increase available privacy-relevant information in order to balance the scale.

In Web communities, for instance, tools for privacy-awareness support can remind individuals about the mass of "quiet users" who are involved in the community only in a passive manner or about the providers of social networks who also have access to data from the profiles such as e-mail addresses, telephone numbers or special interests. To restrict access to contact data helps to keep these personal data items confidential as well as to protect the personal sphere. In this way, no unwanted offers will reach the individual by e-mail, phone or letter.

Further, especially in Web communities people are not only responsible for their own privacy protection. When thinking about relationship-based access control (friends-of-my-friends) to personal profiles or possibilities of putting photos and

videos of others online maybe without their consent, privacy awareness of people should encompass the privacy of persons related to them, e.g. their friends or other persons on the photos and in the videos, as well.

Tools for privacy-awareness support would surely not cover all of those issues, but they aim to prevent uninformed and unintended privacy violations.

4.2 Requirements on Tools to Support Privacy Awareness

For the design of tools that support privacy awareness, a number of requirements emerge and should be considered. In the following section, these requirements are pointed out and explained. Ambivalences, which ensue from the demand for a high flexibility of tools, user-control and freedom of choice for the individual on the one hand and strict definition of rules for implementation on the other hand, are discussed.

- **Measure privacy attitude of people**
  In order to "remind" people about their privacy attitude in specific situations, their general attitude have to be known by the support tool. There are two ways to capture the privacy preferences of people: (a) ask them directly or (b) gather preferences from observation of actual behaviour. The latter option has at least two problems. First, monitoring of the behaviour might be privacy-invasive itself and, second, the privacy paradox describes the gap between attitude towards privacy and behaviour. Hence, drawing conclusions from monitored behaviour would simply not help. Asking people directly means in fact to let them customise their tool for privacy-awareness support. The challenge here is to motivate people to configure and to change preferences, particularly since usually people rarely customise their preferences but rather use default settings 14, 10. Cognitive science refers to this phenomenon as the "status quo bias".

- **No invasion to privacy itself**
  As discussed previously in this paper, privacy means not only minimal disclosure of data to the public, but also minimal interruptions. Thus, the tool for privacy-awareness support should not interrupt its user all time and be annoying to him/her.

- **Understandable for target group**
  The choice of words and descriptions need to be understandable for ordinary people, not only for computer specialists. It is not sufficient to rely on expert opinions about what may be useful to display and how to inform people. As pointed out by Adams and Sasse, it is important to identify and consider the perception, understanding and needs of the target group for designing usable applications 2. The majority of people is not an expert and their level of technical knowledge differs.

- **Consider cognitive boundaries**
  The concept of "bounded rationality", which is well known in cognitive science, signifies the limited ability of individuals to acquire, process, and remember information 20. That is, even if people would theoretically have all privacy-

relevant information available, they will not be able to use all the information for making a rational decision, however they apply a simplified mental model. When designing tools to support privacy awareness this needs to be considered and opportunities have to be researched how to present data to people in a way that they are able to handle it cognitively.

- **Tailored to the specifics of situations**
  Tools to support privacy awareness should influence people's behaviour in concrete situations and therefore need to be user-specific and application-specific. Presentation of information should depend on the current context, i.e., the task, kind of information, recipients, usage, etc. This means either a rule set of all possible contexts has to be defined beforehand by the system's designers or users need to configure their personal sets of contexts, which means making an additional effort for them.

- **Offer support, no assumption of responsibility**
  Tools need to be designed in such a way that they offer support to people. The tools should not convey the impression that they fully protect the privacy of the users according to their preferences or that there is no longer any need for people to be aware of privacy and to take care for themselves.

- **Performance**
  It is essential that tools or features for privacy-awareness support do not decrease performance of the primary application to a perceptible extent, since people will not accept long delays. This is documented for usage of Web sites 9, anonymisation services 13, and it is assumed to be true for privacy-awareness support as a secondary feature as well.

4.3 Opportunities and Limitations of Technical Solutions

Privacy awareness can be supported by several technical tools and mechanisms. Evaluation of privacy metrics or individual privacy preferences and policies are already used as basis for provision of user-specific privacy-awareness features. Privacy Bird 8, for instance, evaluates the matching between the stated privacy preferences of people and Website policies. The tool provides warning signals in case of conflict and thus raises awareness of the user. Indeed, the evaluation process is of what is stated about access to and usage of personal data by the provider of the Website and not how the data really is processed. However, even if actual information processing is considered, the reliability of such tools always depends on the calculations in the background and can only capture technical processing of personal data within the application. For Web communities, not all the information that others would notice and probably store on their own systems individually is ascertainable by metrics and policies. Individuals may find multiple ways of copying information, even if such methods were not technically foreseen, e.g. if a photo sharing community does not offer the option to download photos from others, this does not mean that members cannot take a screenshot of a portrait. In this case, it cannot be guaranteed

that a photo cannot be copied, and the individual cannot even be informed if someone makes a copy. The owner of the photo might get a hint of the possibility that another Internet user can make a copy of the photo before putting it online. However, such warnings carry the risk of not being particularly helpful in increasing privacy awareness in that specific situation; rather they can lead either to ignorance or paranoia. Both should be avoided of course.

5 Conclusions and Future Work

In this paper an introduction to privacy awareness is given. Several studies, mainly from the field of eCommerce, are examined and show the existence of the privacy paradox, i.e., a discrepancy between the stated attitudes of people and their actual behaviour regarding handling of personal data. This also seems to be valid for Web communities where there additionally is a gap caused by the difference between the intended groups of recipients of information and those people who actually can access these data legitimately.

To solve the privacy paradox no solely technical solutions are needed to "protect" people from their own behaviour. People can make informed decisions when not only the benefits of disclosing personal data are pointed out to them, but when they are also reminded about their intentions towards privacy and the existence of possible data recipients. We argue that solutions should also consider cognitive and behavioural aspects by supporting the privacy awareness of people in all online situations. Further, the objective of informed decisions will be facilitated if people are not only aware of the fact that they are going to disclose personal data, but also about the potential consequences. Recent research about transparency enhancing tools (TETs) aims to investigate technical options for providing such information about facts and consequences of disclosure of personal data 11.

The implications of enhanced privacy awareness among Web community members on development of relationships, group awareness and collaborations will be the topic of further research on cognitive and behavioural aspects of privacy and privacy awareness.

Acknowledgements

Many thanks to Stefan Berthold, Rainer Böhme, Hans Hedbom, and Andreas Pfitzmann in particular and my colleagues from TU Dresden in general for inspiration and suggestions to improve this work. I also would like to thank the participants of the IFIP/FIDIS Summer School 2008 for helpful discussions and especially Diane Whitehouse for her comments and improvements of the language.

References

1. Acquisti, A.; Gross, R.: Imagined communities: Awareness, information sharing, and privacy on the Facebook. In: Golle P.; Danezis G. (Eds.): Proceedings of 6th Workshop on Privacy Enhancing Technologies. Cambridge, UK: Robinson College, 2006, pp. 36–58.
2. Adams, Anne; Sasse, Martina Angela: Privacy in multimedia communications: Protecting users, not just data. In: Blandford A.; Vanderdonkt, J. (Eds.): People and Computers XV - Interaction without frontiers. Joint Proceedings of HCI2001, pp. 49–64.
3. Altman, I.: Privacy: A conceptual analysis. In: Environment and Behavior, 8 (1976) 1, pp. 7–29.
4. Awad, Naveen Farag; Krishnan, M. S.: The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. In: MIS Quarterly 30 (2006) 1, pp. 13–28.
5. Birnholtz, J. P.; Gutwin, C.; Hawkey, K..: Privacy in the open: how attention mediates awareness and privacy in open-plan offices. In: Proceedings of the 2007 international ACM Conference on Supporting Group Work (Sanibel Island, Florida, USA, November 04 - 07, 2007). GROUP '07. ACM, New York, NY, pp. 51–60.
6. Chellappa, R. K.; Sin, R. G.: Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. In: Inf. Technol. and Management 6, 2-3 (Apr. 2005), pp. 181–202.
7. Clarke, R.: Introduction to Dataveillance and Information Privacy, and Definitions and Terms. Latest revs. 7 August 2006. Online http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html (last access 2008-07-29).
8. Cranor, L. F.; Arjula, M.; Guduru, P.: Use of a P3P user agent by early adopters. In: Proceedings of the 2002 ACM Workshop on Privacy in the Electronic Society (Washington, DC, November 21 - 21, 2002). WPES '02. ACM, New York, NY, pp. 1–10.
9. Galletta, D. F.; Henry, R.; McCoy, S.; Polak, P.: Web Site Delays: How Tolerant Are Users? In: Journal of the Association for Information Systems, 5, 1 (Jan. 2004), 1–28.
10. Gross, R.; Acquisti, A.; Heinz, H. J.: Information revelation and privacy in online social networks. In: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (Alexandria, VA, USA, November, 2005). WPES '05. ACM, New York, NY, pp. 71–80.
11. Hedbom, Hans: A Survey on Transparency Tools for Enhancing Privacy. In: Pre-Proceedings of the IFIP/FIDIS Internet Security & Privacy Summer School 2008 (Brno, CZ, Sept. 2008), pp. 19-26.
12. Jagatic, T. N.; Johnson, N. A.; Jakobsson, M.; Menczer, F.: Social phishing. In: Communications of the ACM 50, 10 (Oct. 2007), pp. 94–100.
13. Köpsell, Stefan: Low Latency Anonymous Communication - How long are users willing to wait? In: Lecture Notes in Computer Science, Proceedings of Emerging Trends in Information and Communication Security (ETRICS ’06), 3995 (2006) pp. 221–237.
14. Mackay, W. E.: Triggers and barriers to customizing software. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems: Reaching Through Technology (New Orleans, Louisiana, United States, April 27 - May 02, 1991). CHI '91. ACM, New York, NY, pp. 153–160.
15. Manny, C. H.: European and American privacy: Commerce, rights, and justice. In: Computer Law and Security Report, 19 (2003) 1, pp. 4–10.
16. Newell P.B.: Perspectives on privacy. In: Journal of Environmental Psychology, 15 (1995) 2, pp. 87–104.
17. Norberg, Patricia A.; Horne, Daniel R.; Horne, David A.: The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. In: Journal of Consumer Affairs 41 (2007) 1, pp. 100–126.

18. PRIME General Public Tutorial v2. Online available: https://www.prime-project.eu/tutorials/gpto (last access 2008-05-15).
19. Sheehan, K. B.; Hoy, M. G.: Dimensions of privacy concern among online consumers. In: Journal of Public Policy & Marketing 19 (2000) 1, pp. 62–72.
20. Simon, H. A.: Models of bounded rationality. Cambridge, MA: MIT Press, 1982.
21. Spiekermann, S., Grossklags, J., and Berendt, B. 2001. E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In: Proceedings of the 3rd ACM Conference on Electronic Commerce (Tampa, Florida, USA, October 14 - 17, 2001). EC '01. ACM, New York, NY, pp. 38–47.
22. Varian, H.R.: Economic aspects of personal privacy. In: Privacy and Self-Regulation in the Information Age, National Telecommunications and Information Administration, 1996.
23. Warren, Samuel; Brandeis, Louis: The right to privacy. In: Harvard Law Review, 4 (1890), pp. 193–220.
24. Westin, Alan F.: Privacy and Freedom. Atheneum, New York NY, 1967.