Towards Usable Privacy Policy Display & Management - The PrimeLife Approach

J. Angulo[1], S. Fischer-Hübner[2], T. Pulls[2] and E. Wästlund[3]

Karlstad University, Karlstad, Sweden
[1]Department of Information Technologies, [2]Department of Computer Science,
[3]Department of Psychology,
e-mail: {julio.angulo|simone.fischer-huebner|tobias.pulls|erik.wastlund}@kau.se

Abstract

This paper discusses the approach taken within the PrimeLife project for providing user-friendly privacy policy interfaces for the PrimeLife Policy Language (PPL). We present the requirements, design process and usability testing of the "Send Data?" prototype, a browser extension designed and developed to deal with the powerful features provided by PPL. Our interface introduces the novel features of "on the fly" privacy management, predefined levels of privacy settings, and simplified selection of anonymous credentials. Results from usability tests showed that users find some of these features useful and privacy-friendly, and they are therefore suggested as a good approach towards usable privacy policy display and management.

Keywords

PrimeLife Policy Language (PPL), HCI, Usability, Privacy Policy Interfaces.

1. Introduction

When requesting Internet services, users distribute great amounts of personal information at various sites, leaving data traces that can be easily tracked and compiled into extensive personal profiles without them even being aware of it. Article 10 of the EU Data Protection Directive 95/46/EC requires that users are informed about the way their data are handled by different online service providers, implying that users should have the possibility to make conscious informed decisions about the release of their personal data. However, the way service providers express their privacy statements today, usually consists of long texts with complicated legal terms that are often not read or not noticed by users (Kelley et al. 2010).

The PrimeLife EU PF7 project (Privacy and Identity Management for Europe for Life, http://www.primelife-project.eu) aims att developing privacy-enhancing identity management systems for technically enforcing user control and information self-determination. An important prerequisite for supporting users' control in this context is to present transparent and understandable privacy policies. For achieving better transparency, the PrimeLife Policy Language (PPL) allows users to define and adapt their privacy *preferences* declaring under which conditions they would like to release what types of data. PPL also has the capability of comparing the users'

preferences to the privacy policy of service providers, so that users can be informed about the extent to which their privacy preferences will be satisfied.

However, for ordinary computer users, defining and adapting their privacy preferences for properly protecting their privacy online are complex and error-prone tasks which usually require some level of expertise on basic legal privacy concepts and principles. Besides, it is not reasonable to assume that users are willing to spend their time and effort on configuring privacy preferences, specially considering that security and privacy protection are rarely the users' primary tasks (Whitten, Tygar, 1999). In an offline world people manage their privacy preferences more or less automatically, making unconscious choices about the pieces of information they disclose according to the contexts in which they find themselves in at particular times. For example, a person intuitively knows which information is suitable to share with her doctor, but which would be inappropriate to share with her colleagues at work. Thus, the challenge lies in how to translate that instinctive understanding and management of personal privacy to the digital world.

For simplifying the management of privacy preferences, our work in PrimeLife has suggested the novel approach of providing users with predefined *standard* privacy settings which can be customized "on the fly" (i.e. can be modified and saved as a transaction takes place) and to assist them at the moment of selecting certifying attributes that verify their identity. We present the prototype for the "Send Data?" dialog(Figure), a browser extension designed to meet the complex requirements imposed by PPL. The prototype displays the core elements of a service provider's privacy policy in a user-friendly manner and lets users know the extent to which their privacy preferences match the privacy policy of a service provider in situations when their personal data is being requested.

In this paper, we first discuss previous related work on privacy policy management interfaces and on support for users' informed consent in Section 109. Section 3 introduces the capabilities of PPL and identifies the requirements that need to be considered when developing privacy policy management tools for this language. Section 4 describes the design process and usability testing of the "Send Data?" prototype. Conclusions are described in Section 5.

Note that throughout this paper we use the terms *privacy settings* and *privacy preferences* interchangeably. *Privacy preferences* is a well established termed used in P3P and PPL vocabularies, however a study has shown that *privacy settings* is better understood by users in general (Graf et al., 2011). In our interface, however, we consistently used the term *privacy settings*.

2. Related work

For making privacy policies more understandable and transparent, Article 29 Data Protection Working Party (2004) has recommended providing policy information in a multi-layered format. A short privacy notice on the top layer must offer individuals the core information required under Art. 10 EU Directive 95/46/EC, which includes

at least the identity of the service provider and the purpose of data processing. In addition, a clear indication must be given as to how the individual can access the other layers presenting the additional information required by Art. 10, such as information on whether the individual is obliged to reply to the service provider's questions, and on the legal rights of the data subject.

Other previous related work has been done on the usability of P3P (Platform for Privacy Preferences) user agents. The work presented by Cranor, Guduru & Arjula (2006) outlines some of the challenges when designing interfaces for online privacy management, such as the difficulty of users to articulate their privacy preferences and to understand some terminology, as well as the complexity in which the combination of privacy preferences can be presented. The researchers presented a P3P client called "Privacy Bird" and made recommendations for the design of other privacy agents. Reeder (2008) and Reeder et al. (2008) suggest a visualization technique for displaying P3P-based privacy policies based on a two-dimensional grid, declaring an improvement from previous interfaces. Similarly, Kelley et al. (2009) propose a "Nutrition Label" for P3P privacy policies based on the idea that people already understand other nutrition, warning and energy labelling, and claim that their proposed privacy label allows users to find information more accurately and quickly. Nevertheless, P3P has several restrictions, such as the lack of support for downstream data sharing, missing support for stating obligation policies (i.e., policy statements that the service provider promises to fulfil), missing support for anonymous credentials (such as IdeMix credentials (Camenisch, van Herreweghen 2002)), as well as the inability to handle policies from more than one service provider. Other related work, includes the research done by Johnson et al. (2010) on policy authoring and templates, and the work done by Friedman et al. on applying Value Sensitive Design (VSD) to get informed consent from users when managing cookies in web browsers (Millett, Friedman & Felten 2001, Friedman, Howe & Felten 2002). However, these approaches are not fully applicable to European regulations, and are just a part of displaying and managing full privacy policies.

The approach within the PrimeLife project proposes the PrimeLife Policy Language (PPL), which addresses the limitations imposed by P3P, and for which our interfaces have been designed. The work presented in this paper is greatly based on the initial proposals and requirements identified during the PRIME project (Pettersson et al. 2005), and on the previous design iterations presented in PrimeLife deliverables (see PrimeLife WP4.3 (2010)). To the best of our knowledge, no other related work offers standard predefined privacy settings which can be customized semi-automatically "on the fly", assisting users to state their preferred level of privacy depending on the scenario of the transaction. More information about the PrimeLife project, requirements for PPL and other PrimeLife prototypes can be found in (Camenisch, Fischer-Hübner & Rannenberg 2011).

3. Designing for privacy policy management with PPL

During the PrimeLife project, it was seen as a priority to provide user-friendly solutions for managing and displaying understandable privacy policies. The

following section briefly presents some of the features provided by PPL and explains the challenges of designing interfaces for the complexity of this language.

3.1. The challenge of designing interfaces for PPL

Conceptually, PPL can be broken down into three parts: authorizations, obligations and credentials. Taking an attribute-centric view on PPL, for each attribute in a PPL policy the service provider specifies:

- The *purposes* for which the attribute value is requested. For example, requesting authorization to use an email for the purposes of contact and marketing.
- A set of *obligations* it promises to adhere to. Each obligation consists of a set of triggers and an action. For instance, triggers that are activated at a specific time or when the attribute has been accessed for a specific purpose.
- If the attribute needs to be *certified* by any credentials, in IdeMix or X.509 format. The service provider, in the case of IdeMix credentials, may request a proof of predicates over the attribute, and not the actual attribute value, such as proof that the user is over 18-years-old as certified by her identity card issued by the government.

In addition, it is possible for service providers to express in the PPL policy that, for each attribute, it wishes to share data with so-called 'downstream service providers' under specific conditions. Furthermore, PPL allows to specify that a service provider receiving data encrypted by the user with the key of a second service provider should forward that data directly to that second service provider, e.g., if an online shop recieves encrypted payment data which it cannot read, it should forward that data to a payment provider that can decrypt it. This leads to scenarios where there are in fact multiple service providers requesting data from a data subject. Similarly, as when a service provider specifies a PPL policy for a resource, users have PPL preferences set for their attributes and a number of credentials from different issuers stored at their local PPL engine. When a user wants to access a resource her preferences are matched with the PPL policy specified by the service provider. The result of this match can be sent to a graphical user interface (which proposed design is described in Section 4) allowing the user to make an informed decision about the disclosure of her data. Note, however, that the complexity and variety of features provided by PPL poses challenges when trying to capture all this information inside a user interface, while at the same time trying to keep the interface as user friendly and understandable as possible.

3.2. Identified requirements for a privacy policy management interface

We present here some of the requirements that have been identified as necessary for providing privacy policy interfaces that will support the users' control over their personal information using the PPL engine.

For displaying the policy information required by Art. 10 EU Directive 95/46/EC in a more transparent manner as a basis for obtaining users' informed consent to data disclosures, we are in particular following the Art. 29 Working Party's recommendation of displaying policies in multiple layers (Art.29 2004).

Furthermore, the interface must assist users at selecting one combination of credentials for certified attributes and, if necessary, allow them to fill in values for uncertified attributes. The PPL engine can populate the interface with all possible combinations of a user's credentials so that users can select the combination of credentials that fit the data request in question.

Users should also be informed about the possible policy mismatches in a not too alarming manner, letting them take rational decisions on how to proceed. In case of a mismatch, users should be allowed to customize their current privacy settings "on the fly" by having the option of overruling their settings for the current transaction only or for all future transactions. In addition, the interface should also provide users with documentation and feedback information on the different aspects of the interface that will help clarify its intentions. Since the concept of online privacy is not simple to understand, it is at times necessary to assist users in an unobtrusive manner. It was also detected in previous studies that users often have difficulties in differentiating between the information being handled locally on their computer and the one handled on the service provider's side (Pettersson et al. 2005), thus it is also important that the interface helps users to see this difference so that they understand that policy matching and preference management takes place locally under the users' control.

4. Designing the "Send Data?" browser extension

Having identified the requirements listed above, a Firefox plug-in prototype for privacy policy management called "Send Data?" was conceptualized and developed. An iterative process of design was adapted in which users' feedback was considered at every iteration cycle. The version of the "Send Data?" dialog presented in this paper (Figure 1) corresponds to the sixth iteration cycle. More detailed descriptions of earlier iterations and the evolution of the dialog have been presented by Pettersson et al. (2005), PrimeLife WP4.3 (2010) and Angulo et al. (2011). Figure 1 presents the latest design proposal corresponding to the seventh iteration cycle.

4.1. User Interface elements and the rationale behind design decisions

The interface of the "Send Data?" dialog is divided into a top and a bottom panel (Figure 1). When the dialog pops up, the website behind it is dimmed and the address bar is coloured, helping users understand that the dialog works on the client side and is not part of the service provider, thus fulfilling one of the requirements above.

The top panel includes a two-dimensional table initially adapted from the visualization technique for P3P policies suggested by Kelley et al. (2009). However, in our design, the table was adapted to meet the previous listed requirements and to

take advantage of the additional features provided by PPL. One important adaptation in our version of the table was the removal of the icons within each cell, since earlier tests showed that users interpreted them as clickable buttons. In our version of the table, the purposes for which the users' data will be employed are represented by the table's columns, whereas the types of information requested are listed in the rows. In the leftmost column the user can select the credentials that certify the attributes requested by the service provider and enter values for uncertified attributes. The selection of certified credentials is done using the card-based metaphor for credential selection described in the PrimeLife deliverable WP4.1 (2010).

In contrast to the work presented by Kelley et al. (2009) our prototype lets users recognize which service providers are requesting which kind of information thanks to PPL capability of displaying policies from multiple service providers.

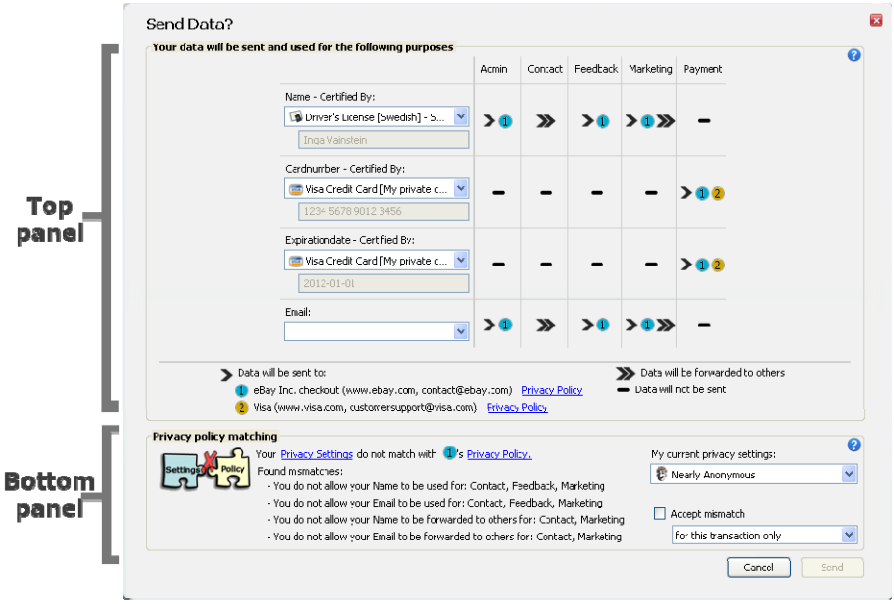

Figure 1: The look-and-feel of the prototype of the "Send Data?" dialog

When a service provider requests information to be used for a particular purpose, an arrow pointing to a circled number appears in the corresponding cell. In the version presented here, colour was added to the circled numbers in order to create a stronger visual connection between the table and the list of service providers ➤1. Furthermore, a *forwarding arrow* icon ➤➤ informs the users when a policy states that their data will be downstreamed to third parties and for which purposes. This is yet one more addition to the grid proposed by Kelley et al. (2009) where users are not informed about the purposes of downstream data usage.

The bottom panel of the dialog is subdivided into three parts. The bottom *left* part shows a puzzle piece icon, representing a "match" or "mismatch" between the users'

privacy settings and the service providers' privacy policies. The idea is to provide users with quick visual feedback which is not perceived in a too alarming manner and which makes use of the users' peripheral vision. The *middle* part, lists all the found mismatches, and also, as listed in the legal requirements, provides a link to the full privacy policy of the service provider, fulfilling the recommendation of displaying policies in multiple layers.

The bottom *right* part of the dialog (Figure 2) displays UI-controls allowing users to change their privacy settings semi-automatically "on the fly". With this is a novel approach users can define their privacy preferences at the moment a transaction takes place by selecting a predefined *standard* level of privacy ("Nearly anonymous", "Minimum data" and "Requested data") and having the possibility of overruling their settings for the current transaction only, to update their settings for all future transactions or to adapt their settings for future transactions and save them under a new name.

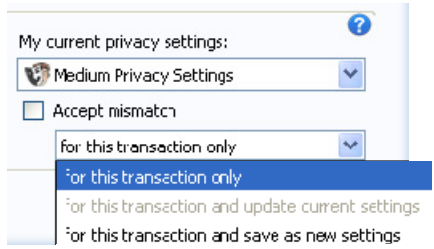

Figure 2: "On the fly" privacy management

We expected that with the use of this interface, users would be able to make more informed decisions and conscious choices about the release of their personal information. Users are, however, left in control of the final decision on whether continuing or cancelling an online transaction, and are given the option to modify their privacy preferences for current and future transactions.

4.2. Usability Testing of "Send Data?"

The version of the "Send Data?" dialog presented here was tested with 10 participants (mostly students) at Karlstad University (KAU) in Sweden, and 14 more participants at CURE (Center for Usability Research and Engineering) in Austria, all coming from different cultural and educational backgrounds. A Cognitive Walkthrough approach, questionnaires and Eye-tracking techniques were used as means of gathering the opinions of the participants. During a test session participants were asked to complete a series of tasks and answer questions while interacting with the prototype. For example, participants were asked to mention the *purposes for which their name was being requested*; similarly, they were given the task to *modify the privacy settings so that they would agree with the policy of the service provider for future transactions*. At the same time, they were encouraged to express their general understanding of the dialog and to give their opinions on different interface

elements. Afterwards, they were asked to fill in a PET-USES questionnaire (Wästlund, Wolkerstorfer & Köffel 2010).

4.2.1. Relevant results and suggestions for improvement

This section presents the evaluation results and suggestions for improvement based on the feedback obtained from participants and other spotted usability problems. The improvements have been implemented for the interface of the next iteration cycle, shown in Figure 3

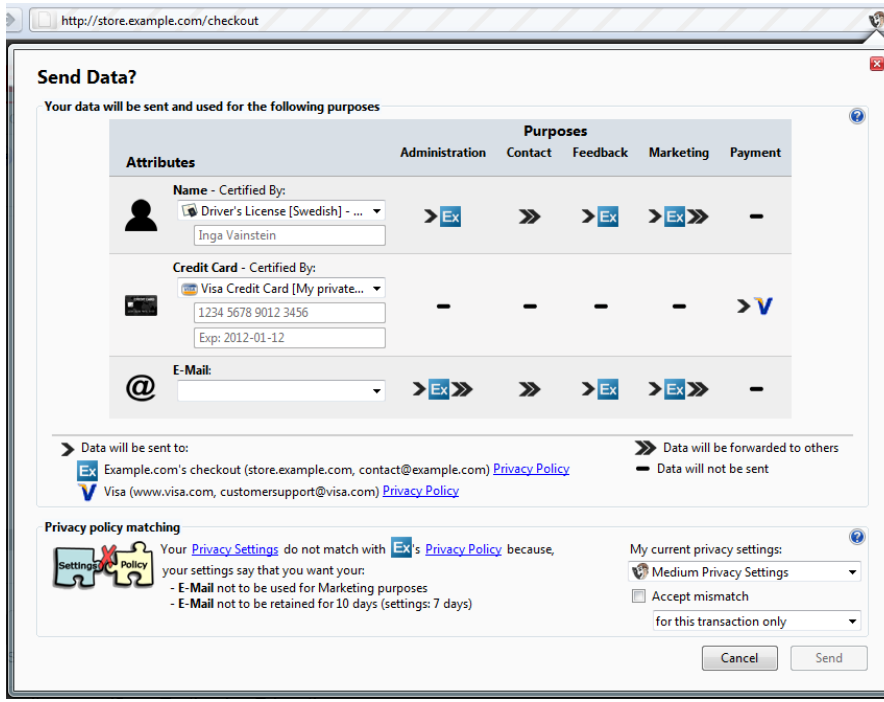

Figure 3: A redesign suggestion for the seventh iteration cycle

In general, results from the tests showed that participants understood that the "Send Data?" dialog protects their privacy by showing them when their privacy settings do not match with a privacy policy, and that the dialog was not part of a service provider by popping-up on top of the website and dimming the background. Participants also appreciated the possibility to manage privacy settings "on the fly", although some were confused by the labels used in the predefined levels of privacy ("Nearly anonymous", "Minimum data" and "Requested data"). It was suggested renaming the labels to "High privacy", "Medium privacy" and "Low privacy".

14 out of the 24 participants in total clearly and quickly understood the purposes for which their information was being requested with the help of the table. To account for the percent that did not understood so clearly, a suggestion has been made to

include the title "Purposes" above the columns and making the columns' headings more prominent, since the main problem was caused by poor visibility.

6 out of 24 participants expressed, in some way or another, their wish to visualize the *mismatches* within the table or interpreted the table as being a representation of their own privacy settings. It was observed that the table, which is basically a summary of the service providers' privacy policies, can also help users perceive a mismatch if they have their privacy settings in mind. However, the bottom panel provides a more user-friendly visual representation of mismatches, following the usability heuristic of "recognition rather than recall". Augmenting the table with information in the form of tooltips has been suggested as a way to give users a better idea of the data being requested and for which purposes.

In the credential selection part, 8 out 10 participants at KAU understood that only the attributes of each credential were sent to the service provider, and not the credential itself. It has been suggested to add improvements to the table so that credentials are better organized and recognized by users. For example, having different colours for each row (credential) in order to differentiate them visually, as well as representing credentials with icons familiar to users.

Eye-tracking data showed that participants made visual connection between the coloured circled numbers inside the table (e.g., ➤❶) and the list representing the service providers at the bottom. Further improvements have been suggested so that the logo of the service provider is shown instead of circled numbers (➤Ex). In case the service provider has no logo available, the circled numbers approach would be used. Regarding the mismatching puzzle-piece icon, 7 out of 10 participants at KAU stated that they understood the intention of the icon. Eye-tracking data also revealed that participants usually avoided reading the list of found mismatches (i.e., middle bottom part), presumably due to too much text. Suggested improvements include rewording the mismatches (considering obligation mismatches) and bolding the attributes so that users get an idea of the reason of the mismatch in a quicker way.

Figure 3 shows the redesign of the dialog based on the results from the usability test. The interface was modified by improving the readability of the two-dimensional table with the use of alternating row colours, prominent headers and showing service providers' logos. The process of selecting credentials will presumably become simpler with the new regrouping of attributes and icon representations. Also, the new labelling of the predefined standard privacy settings is now more self-explanatory, and found mismatches would expectantly be better understood by users.

5. Conclusions

The features provided by the PrimeLife Policy Language (PPL) are very powerful, but at the cost of added complexity. Arguably, applying user-friendly interfaces for this language is more complicated than for other simpler policy languages, such as P3P. Our results from usability testing show that users understand the core aspect of the proposed "Send Data?" dialog, but still have some difficulties understanding the

whole concept of online privacy policy management. Improvements are still needed and a final round of testing will unveil the usability of the design for the last iteration cycle. Nevertheless, the novel concept of "on the fly" privacy settings seems to be a promising approach towards usable privacy policy interfaces. In the future, additional tests will be carried out on the new proposed interface to detect the usability problems that still exist and the ones that have been resolved.

6. Acknowledgments

Research leading to these results was partly funded as a Google Research Award project. Funding was also received from the EU 7th Framework programme (FP7/2007-2013) for the PrimeLife project.

7. References

Angulo, J., Fischer-Hübner, S., Pulls, T. & König, U. 2011, "HCI for Policy Display and Administration" in *PrimeLife - Privacy and Identity Management for Life in Europe*, Springer, pp. 261.

Art.29 Working Party 2004, *Opinion on More Harmonised Information Provisions 1198704/EN WP 100*, European Commission.

Camenisch, J., Fischer-Hübner, S. & Rannenberg, K. (eds) 2011, *PrimeLife - Privacy and Identity Management for Life in Europe*, 1st edn, Springer.

Camenisch, J. & van Herreweghen, E. 2002, "Design and implementation of the IdeMix anonymous credential system", *Proceedings of the 9th ACM conference on Computer and Communications Security*, pp. 21.

Cranor, L.F., Guduru, P. & Arjula, M. 2006, "User interfaces for privacy agents", *ACM Trans.Computer-Human Interaction,* vol. 13, no. 2, pp. 135-178.

Friedman, B., Howe, D. & Felten, E. 2002, "Informed consent in the Mozilla browser: Implementing value sensitive design", Published by IEEE Computer Society, pp. 247.

Graf, C., Wolkerstorfer, P., Hochleitner, C., Wästlund, E. & Tscheligi, M., 2011, "HCI for PrimeLife Prototypes" in *PrimeLife - Privacy and Identity Management for Life in Europe*, eds. J. Camenisch, S. Fischer-Hübner & K. Rannenberg, Springer, pp. 217.

Johnson, M., Karat, J., Karat, C. & Grueneberg, K. 2010, *Optimizing a policy authoring framework for security and privacy policies*, ACM, Redmond, Washington.

Kelley, P.G., Cesca, L., Bresee, J. & Cranor, L.F. 2010, "Standardizing privacy notices: An online study of the nutrition label approach", *Proceedings of the 28th international conference on Human factors in computing systems.* ACM, pp. 1573.

Kelley, P.G., Bresee, J., Cranor, L.F. & Reeder, R.W. 2009, "A 'Nutrition Label' for Privacy", *SOUPS '09: Proceedings of the 5th Symposium on Usable Privacy and Security*. ACM, New York, NY, USA.

Millett, L.I., Friedman, B. & Felten, E. 2001, "Cookies and Web browser design: toward realizing informed consent online", *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, pp. 46.

Pettersson, J.S., Fischer-Hübner, S., Danielsson, N., Nilsson, J., Bergmann, M., Kriegelstein, S.C.a.T. & Krasemann, H. 2005, "Making PRIME usable", *Proceedings of the 2005 Symposium on Usable Privacy and Security*. ACM, New York, NY, USA, pp. 53.

PrimeLife WP4.1 2010, "High-level Prototypes", *PrimeLife Deliverable D4.1.4*, eds. C. Graf, P. Wolkerstorfer, E. Wästlund, P. Wolkerstorfer, S. Fischer-Hübner & B. Kellermann, PrimeLife (http://www.primelife.eu/results/documents), August.

PrimeLife WP4.3 2010, "UI Prototypes: Policy Administration and Presentation -- Version 2", *PrimeLife Deliverable D4.3.2}*, eds. S. Fischer-Hübner & H. Zwingelberg, PrimeLife (http://www.primelife.eu/results/documents), June.

Reeder, R.W. 2008, *Expandable grids: a user interface visualization technique and a policy semantics to support fast, accurate security and privacy policy authoring*, Carnegie Mellon University.

Reeder, R.W., Bauer, L., Cranor, L.F., Reiter, M.K., Bacon, K., How, K. & Strong, H. 2008, "Expandable grids for visualizing and authoring computer security policies", *Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems.* ACM, New York, NY, USA, pp. 1473.

Wästlund, E., Wolkerstorfer, P. & Köffel, C. 2010, "PET-USES: Privacy-Enhancing Technology - Users' Self-estimation Scale" in *Privacy and Identity Management for Life*, Springer Boston, pp. 266-274.

Whitten, A. & Tygar, J.D. 1999, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0", *Proceedings of the 8th USENIX Security Symposium*.