Towards Usable Privacy Policy Display & Management for PrimeLife

Julio Angulo¹, Simone Fischer-Hübner², Tobias Pulls² and Erik Wästlund³

Karlstad University, Karlstad, Sweden
¹Department of Information Technologies, ²Department of Computer Science, ³Department 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 understand and appreciate these features and perceive them as being privacy-friendly, and they are therefore suggested as a good approach towards usable privacy policy display and management. Additionally, we present our lessons learn in the design process of privacy policy interfaces.

Keywords

PrimeLife Policy Language (PPL), usability, privacy policy interfaces.

1. Introduction

The number of services available on the Internet has increased considerably in the last decade and it is expected to continue rising in the following years. When requesting Internet services, users tend to 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 understood 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 at 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 policies 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, since 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 an online 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, 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. We also report about the lessons learned during the design process and recommendations for the design of other usable policy interfaces.

In this paper, we first discuss previous related work on privacy policy management interfaces and on support for users’ informed consent in Section 2. Section 3 introduces the capabilities of PPL and the requirements that we identified as important to consider when developing privacy policy management tools for this language. Section 4 describes the design process and usability testing of the “Send Data?” prototype. Discussions and lessons learned are presented in Section 5. Finally conclusions are drawn in Section 6.

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

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.

Previous related work has been done on the usability of P3P (Platform for Privacy Preferences) user agents. For instance, 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 only cover some aspects 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) and PrimeLife WP4.1 (2011)). 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
The following section briefly presents some of the features provided by PPL and explains the challenges and requirements for 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, PPL makes it possible for service providers to express the sharing of users’ data with ‘downstream service providers’ (i.e., third party entities requesting data attributes) 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 the data directly to that second service provider. For instance if an online shop receives encrypted payment data which it cannot read, it should forward that data to the corresponding payment provider that can decrypt it. This leads to scenarios where there are in fact multiple service providers requesting data from one data subject during one transaction.

Similarly, as when a service provider specifies a PPL policy for a resource, PPL allows users to specify their preferences for each of their attributes and a number of credentials from different issuers stored at their local PPL engine. When users want to access a resource, their 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, allowing users to make an informed decision about the disclosure of their 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. Our attempt to tackle these challenges resulted in the interfaces described in Section 4.

3.2. Identified requirements for a privacy policy management interface

We present here some of the requirements that we have identified as necessary for providing privacy policy interfaces for the PPL engine that will support the users’
control over their personal information. This requirements are partly grounded on our previous experiences working with privacy policy interfaces.

First, 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 users’ credentials so that users can select the combination of credentials that fit the data request for the transaction at hand.

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. However, users should not be encouraged to easily change their settings in order to get rid of the warnings. Instead the interface should make users consciously aware of the data they are about to release.

In addition, it is important that the interface helps users differentiate between the information being handled locally on their computer and the one handled on the service provider’s side, since previous studies have shown the difficulties users have to notice this difference (Pettersson et al. 2005).

Finally, 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.

4. Designing the “Send Data?” browser extension

Having identified the requirements listed above, a prototype for privacy policy management called the “Send Data?” dialog was conceptualized and developed as a Firefox plug-in. An iterative process of design was adapted in which users’ feedback was considered at every iteration cycle. Based on the results from usability tests of the sixth iteration cycle (Figure 1) presented in Angulo et al. (2011b), we present a redesign and an alternative design corresponding to the seventh iteration cycle in the following sections (shown in Figure 2 and Figure 5 respectively). More detailed descriptions of earlier iterations and the evolution of the dialog have been presented by Pettersson et al. (2005), PrimeLife WP4.3 (2010), PrimeLife WP4.3 (2011) and Angulo et al. (2011a).
Figure 1. The interface for the earlier sixth iteration cycle of the “Send Data?” dialog.

4.1. User Interface elements and rationale behind design decisions

The interface of the “Send Data?” dialog is divided into a top and a bottom panel. The top panel, which reads “Your data will be sent and used for the following purposes”, includes a two-dimensional table initially inspired 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. In our version of the table, the purposes for which the users’ data will be used are represented by the table’s columns, whereas the types of information requested (attributes) are listed in its 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 as 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. An arrow pointing to the logotype of the service provider, ➔, appears in the corresponding cell, indicating that a service provider is requesting to be used for a particular purpose (for example, in a real transaction the logo of eBay, Amazon.com, etc. would appear). A forwarding arrow icon ➔ informs the users when a policy states that their data will be forwarded to third parties and for which purposes it will be
sent. 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, with the title “Privacy policy mismatching”, 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 that is not perceived in a too alarming manner. The middle part, lists all the found mismatches, and also, as mentioned in the legal requirements, provides a link to the full privacy policy of the service provider, fulfilling Art. 29 recommendation of displaying policies in multiple layers. An earlier design decision was made to show the existing mismatches separated from the two-dimensional table, since it was difficult to display all kind of mismatches within the table, such as obligation mismatches.

Figure 2. The look-and-feel of the seventh iteration cycle

The bottom right part of the dialog (also shown in Figure 3) displays UI-controls allowing users to change their privacy settings semi-automatically “on the fly”. With this novel approach users can define their privacy preferences at the moment a transaction takes place by selecting a predefined standard level of privacy (“High Privacy Settings”, “Medium Privacy Settings” and “Low Privacy Settings”) 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. Given that most users rarely want to be bothered with adjusting their privacy settings (PrimeLife WP4.1 2011), our
approach is to start with a privacy-friendly value as default (i.e., “High Privacy Settings”) and let users adapt this settings in an appropriate context.

![Figure 3. "On the fly" privacy management](image)

Being a Firefox plug-in, we adapted the look-and-feel of the dialog to match that of other components of this web browser, making its behaviour more consistent and recognizable by users. When a transaction takes place, the website requesting data is dimmed in the background and the address bar is striped as soon the dialog pops up. This helps users understand that the dialog runs on the client side and is not part of the service provider’s website, thus fulfilling one of the requirements listed in Section 3.2. Also, users are given the opportunity to adapt their level of privacy for a particular service provider directly on the address bar, in a similar fashion as they would bookmark a website (see Figure 4), making the management of privacy settings more accessible.

![Figure 4. "On the fly" privacy management directly on the address bar](image)

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 “on the fly”.

4.2. Alternative design for the seventh iteration cycle

For the seventh iteration cycle an alternative design was proposed, shown in Figure 5. The purpose of this alternative design is to address some of the critical usability pitfalls encountered in the previous tests of earlier iteration cycles, but which full implementation would be time consuming and difficult to achieve given the
complexity and restrictions of PPL, such as displaying obligations and other mismatches inside the table, and making the table’s cells interactive.

The alternative design was conceptualized as an interactive mock-up with the use of Karlstad University’s Ozlab system (Pettersson 2003, Pettersson, Siponen 2002). The Ozlab system is an implementation of the Wizard-of-Oz technique, commonly used within the field of interaction design to investigate the usability of interactive systems before creating high-definition prototypes or fully developed products. We decided to make use of the Ozlab system since it provides a quick and cheap way to suggest changes to a design and carry out usability tests. The following paragraphs illustrate the additions made to the alternative design with the use of Ozlab system to try to address these issues.

First of all, a preliminary study was made at Karlstad University on the effect that the use of colour could have for displaying privacy policies mismatches. Results indicated that the use of the colour red can be effective at capturing the attention of users and making it easier to recognize mismatches. The use of colour was also an important part of the privacy agent suggested by Cranor et al. (Cranor, Guduru & Arjula 2006, Cranor 2003), the Privacy Bird, where a red coloured bird icon indicates that the users’ privacy settings do not match a website’s P3P policy, and the green colour indicates a match. Based on these studies and results, we introduced colours inside the table’s cells, using red to represent that a mismatch for each of the attributes being requested for a particular purpose, and a faded colour green to represent a match. We decided to discretely place these colours on the top of each cell trying not to disrupt the visual appearance of the dialog, and keeping the requirement of presenting mismatches in a not too alarming manner. With the use of these colours, users would not only be able to see if a mismatch exists or not, but they could even have a quick way to identify the particular setting that is not matching with a part of the policy.

Furthermore, we added an interactive aspect to the table by letting users click on the different cells containing a mismatch, which shows the mismatch information specific to that cell on the middle part of the bottom panel. The list of mismatches that used to be shown on that bottom middle part in the previous design suggestions was removed in order to avoid visual clutter, and since previous eye-tracking tests revealed that most participants did not read them. Instead, users could click on a link that would show all found mismatches when they choose too. Also, a slightly faded mismatch icon (i.e., two puzzle pieces not fitting together) was subtly displayed in the background of a mismatching cell, presumably helping users understand the nature of the mismatch and where they could find more information.

We also added a column representing obligations, called “Conditions”, and try to represent these kind of policies with privacy icons developed under the PrimeLife project (Holtz, Nocun & Hansen 2011). For instance, in the test scenario we had the

---

1 The study was made by Anna Oskarsson’s Master Thesis “How color can affect the usability of graphical interfaces in programs that handle users’ privacy” for the Department of Information Systems at Karlstad University.
obligation that the service provider must delete the user’s data after ten days, represented by a garbage bin icon and the number of days (see rightmost column on Figure 5).

4.3. Usability testing of the seventh iteration cycle

A usability evaluation for the seventh iteration cycle was carried out at Karlstad University with 10 test participants, 7 women and 3 men ranging from 26 to 57 years of age, coming from different cultural and professional backgrounds. A Cognitive Walkthrough approach was used to get the opinion of participants on the two variants of a similar design: the implemented Firefox plug-in and the Ozlab interactive mock-up. A comparison test was employed in which 5 of the participants performed the test based on the Firefox plug-in prototype, and at the end they were shown the Ozlab mock-up and asked to state their preferences. The other 5 participants were shown the Ozlab mock-up first and then the implemented prototype.

Results showed a general improvement over the earlier version of the sixth iteration cycle presented by Angulo et al. (2011b). In particular, the collected data shows that the use of the service provider’s logotypes inside the cells made it easier for users to recognize who were the service providers requesting data. Also, participants had no trouble identifying the credentials that verify their attributes and understanding the pieces of data that would be sent to the service providers, suggesting that grouping the credentials by coloured rows and including representative icons is a good approach for credential selection. Consistent with earlier tests, all participants clearly understood that the dialog pops-up before any of their data is being sent to the service provider.

Nevertheless, contrary to our expectations, the understanding of the purposes for which data was being requested did not seem to improve by much, even when the headers were made more prominent. Also, none of the participants noticed the help of tooltips containing information on each cell. Curiously enough, half of the participants commented that there were “too many arrows” and symbols that were not visually pleasant (i.e., and ), when earlier tests did not exhibit this problem. Our guess is that introducing the service providers’ logos within the table created confusion, making participants visually overwhelmed with too many icons.

All of the participants who were shown the Ozlab mock-up first (Figure 5), clearly understood that a service provider was requesting data that did not agree with their privacy settings. All of them mentioned the red stripe on the cell and the mismatching icon in the background as the rationale behind their response. However, it seems that the interactive aspect of the table in the Ozlab version was not intuitive enough, since only one of the participants clicked on the cells in order to find more information about a mismatch. The “Conditions” column was also not easy to understand, presumably due to the fact that users are often not aware of privacy policies containing obligations.
Figure 5. An alternative redesign for the seventh iteration cycle

When asked which of the two alternatives they would prefer to install on their computers in order to protect their privacy 9 out of 10 participants answered in favour of the coloured Ozlab mock-up, arguing that it makes it easier for them to recognize a mismatch and that it has a cleaner look-and-feel. The remaining participant did not have any preference over the two alternatives.

5. Discussions and lessons learned

From our various iterative cycles of the design of the “Send Data?” dialog we consider the following factors as important when designing interfaces for privacy policy display and management, which supplement our previously identified requirements presented in Section 3.2.

First of all, the idea of being able to manage their privacy “on the fly” seems to be appealing for users and also easy to grasp. This feature helps users protect their privacy by making it easier for them to change their levels of privacy, which is a task that users seldom want to be bothered with.

Congruent with the observations from Kelley et al. (2009), the use of textual descriptions in an interface made for privacy policy display brings little value to its usability. Using visual representations when appropriate, such as suitable icons and symbols, is encouraged. However, finding the right visual representations that most users will understand is not always a trivial task. Our evaluations showed that users tended not to look at areas where plenty of text was displayed, but they also became
overwhelmed if many icons were clustered together, as was the case when placing arrows and logotypes inside a cell in the table.

If used appropriately, the subtle use of colour can help convey meaning in a good way. In our earlier versions of the “Send Data?” dialog the use of red and blue coloured icons were used inside each cell to represent that data would be sent or not (PrimeLife WP4.3 2010). In that case, the table captured the users’ attention immediately, making them alarmed when too many red icons were displayed and stealing their attention from the other parts of the interface. In our latest design suggestion (Figure 5) discrete coloured stripes were used, achieving better results and conveying the desired meaning.

Moreover, the representation of obligations in the interface is still a challenge. Our suggestion of placing a column besides the table to represent obligations created confusion among test participants, probably due to the fact that users are not familiar with the concept of obligations in privacy policies. A better and more intuitive way to display these kind of mismatches is still needed that can help no-privacy expert users understand this concept.

Throughout our different iterations, it was observed that users need some time to interact with the “Send Data?” interface before grasping the idea that it is trying to convey. When being presented with the dialog for the first time, test participants tended to be confused by the different aspects of the interface, but by the end of the usability test they were able to understand its purpose and benefits to their privacy. This might be due to the fact that users are still unfamiliar to interfaces that try to protect their privacy, but short explanations and analogies are enough to help them get the idea of the dialog. Therefore, conveying one-time informative hints on the different aspects of the interface might help users understand the elements of the program and how it can help them protect their privacy.

6. Conclusions

The PrimeLife Policy Language (PPL) provides very powerful features, but at the cost of added complexity when it comes to usability. Arguably, applying user-friendly interfaces for this language is more complicated than for other policy languages, such as P3P. Our results from usability testing show that users understand the core aspect of the “Send Data?” dialog proposed hereby, and that improvements to its interface have been achieved at every iteration cycle. Nevertheless, some improvements are still necessary in order to make the interaction and representation of information more intuitive. From our results, it also became clear that the use of colours in a two-dimensional table is a good approach towards representing mismatches of the users’ privacy preferences and service providers’ privacy policies, corroborating to some extent the findings by Kelly et al. (2009). Moreover, the novel concept of “on the fly” privacy settings seems to be understood and appreciated by users, as well as the selection of credentials using a card-based approach clearly grouped by rows. From our experience working through the different design cycles of the dialog we have reported our lessons learned and suggestions for designing other privacy policy interfaces.
Despite the improvements made so far, there are still challenges to be tackled, especially when thinking about future interaction paradigms, such as displaying user-friendly privacy policies in mobile smart devices with restricted screen sizes, or obtaining informed consent from users in the era of ubiquitous computing where interconnected devices will be practically invisible and interaction might occur without the use of visual interfaces. These are issues that should be addressed in order to provide privacy-friendly online services in the near future.

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.

References


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.
